GFI Product Manual

GFI MailEssentials™

Administrator- und Konfigurationshandbuch





http://www.gfi.com

info@gfi.com

Die Informationen in diesem Dokument dienen ausschließlich Informationszwecken und werden in der vorliegenden Form ohne (ausdrückliche oder stillschweigende) Haftung jeglicher Art bereitgestellt, insbesondere ohne Gewährleistung der Marktgängigkeit, der Eignung für einen bestimmten Zweck oder der Nichtverletzung von Rechten. GFI Software haftet nicht für etwaige Schäden, einschließlich Folgeschäden, die sich aus der Nutzung dieses Dokuments ergeben. Die Informationen stammen aus öffentlich zugänglichen Quellen. Trotz sorgfältiger Prüfung der Inhalte übernimmt GFI keine Haftung für die Vollständigkeit, Richtigkeit, Aktualität und Eignung der Daten. Des Weiteren ist GFI nicht für Druckfehler, veraltete Informationen und Fehler verantwortlich. GFI übernimmt keine Haftung (ausdrücklich oder stillschweigend) für die Richtigkeit oder Vollständigkeit der in diesem Dokument enthaltenen Informationen.
Nehmen Sie mit uns Kontakt auf, wenn Ihnen in diesem Dokument Sachfehler auffallen. Wir werden Ihre Hinweise sobald wie möglich berücksichtigen.
Alle hier aufgeführten Produkte und Firmennamen sind Marken der jeweiligen Eigentümer.
GFI MailEssentials unterliegt dem urheberrechtlichen Schutz von GFI SOFTWARE Ltd. – 1999–2011 GFI Software Ltd. Alle Rechte vorbehalten.
Version ME-ACM-DE-1-02.010
Letzte Aktualisierung: 5. September 2011

Inhalt

Abbildungsverzeichnis

1 Einführung

GFI MailEssentials ist eine Server-Anti-Spam-Lösung, die Ihren Mailserver durch wichtige Anti-Spam-Funktionen für Firmen-E-Mail ergänzt. Als Zusatz zu Ihrem Mailserver ist GFI MailEssentials komplett benutzertransparent, eine zusätzliche Schulung der Benutzer ist nicht erforderlich.

Haupteigenschaften dieser Lösung:

- **Servergestützte Anti-Spam-Lösung** - Spamschutz ist ein wichtiger Teil der Sicherheitsstrategie für Ihr Netzwerk. GFI MailEssentials bietet moderne Spam-Filter, beispielsweise mit Blockliste und Whitelist, Bayes-Filter, Keyword-Prüfung und Header-Analyse.
- **Quarantäne** - Eingehende Spam-E-Mails verbleiben für einige Tage in einem zentralen Speicher. Dies vereinfacht die E-Mail-Verwaltung und reduziert die verwendeten Ressourcen für die Verarbeitung auf dem Mailserver.
- **Unternehmensweit einheitlicher Haftungsausschluss und Fußzeilentext -** Unternehmen haften für den Inhalt der E-Mail-Mitteilungen ihrer Mitarbeiter. Mit GFI MailEssentials können Haftungsausschlüsse automatisch am Anfang oder Ende einer E-Mail eingefügt werden, ebenso Felder und Variablen, die den Haftungsausschluss für den Empfänger entsprechend anpassen.
- **Berichterstellung -** GFI MailEssentials kann verschiedene nützliche Berichte zur Nutzung von E-Mail und zur Spam-Bekämpfung erzeugen.
- **Personalisierte automatische Antworten mit Referenznummer** - Automatische Antworten können nicht nur mitteilen, dass gerade niemand im Büro ist, sondern den Kunden informieren, dass seine E-Mail eingegangen ist und die Anfrage beantwortet wird. Ordnen Sie jeder Antwort eine eindeutige Referenznummer zu, damit Kunden und Mitarbeiter Nachrichten einfacher finden.
- **POP3-Downloader -** Kleinunternehmen haben möglicherweise nicht die entsprechenden Systeme zur Nutzung von SMTP-E-Mail. GFI MailEssentials enthält ein Modul, das E-Mails von POP3-Postfächern abrufen und in Postfächer auf dem Mailserver verteilen kann.
- **E-Mail-Überwachung** - Zentrale Datenspeicher lassen sich in der Regel einfacher verwalten als verteilte Informationen. GFI MailEssentials erlaubt für die E-Mail-Nachrichten einer bestimmten Person oder Abteilung den Versand von E-Mail-Kopien an einen zentralen Speicher.

Weitere Informationen zur Filterfunktion von GFI MailEssentials für eingehende und ausgehende E-Mails finden Sie in Informationen zu GFI MailEssentials in diesem Handbuch

1.1 Verwendung dieses Handbuchs

Dieses Benutzerhandbuch ist eine ausführliche Anleitung, die die Systemadministratoren bei Konfiguration und Nutzung von GFI MailEssentials möglichst umfassend unterstützen soll. Dieses Handbuch baut auf den Hinweisen auf, die Sie in der 'Kurzanleitung für GFI MailEssentials' finden und beschreibt die Konfigurationseinstellungen, die Systemadministratoren vornehmen müssen um die Software optimal zu nutzen.

1.2 Glossar

Active Directory	Ein Verfahren mit verschiedenen Netzwerkdiensten beispielsweise LDAP-ähnlichen Diensten
AD	*Siehe* Active Directory
Automatische Antwort	Eine E-Mail-Antwort, die automatisch nach Eingang einer E-Mail versendet wird.
Bayes-Filter	Ein Spamverfahren, bei dem nach Training durch die Benutzer Spam-Mails mit statistischen Verfahren identifiziert werden.
BITS	*Siehe* Intelligenter Hintergrund-Übertragungsdienst
Blockliste	Ein Verzeichnis der E-Mail-Benutzer beziehungsweise Domänen, von denen Benutzer keine E-Mails erhalten sollen.
Botnet	Eine Schadsoftware, die autonom und automatisch läuft und von einem Hacker/Cracker gesteuert wird.
CIDR	*Siehe* Classless Inter-Domain Routing
Classless Inter-Domain Routing	Eine Notation für IP-Adressen zum Festlegen eines IP-Adressbereichs.
Demilitarisierte Zone	Ein Bereich des Netzwerks, der nicht Teil des internen Netzwerkes ist, aber auch kein direkter Teil des Internets. Sie dient im Prinzip als Gateway zwischen internen Netzwerken und dem Internet.
DMZ	*Siehe* Demilitarisierte Zone
DNS	*Siehe* Domain Name System
DNS MX	*Siehe* Mail Exchange
Domain Name System	Eine Datenbank in TCP/IP-Netzwerken, die die Übersetzung von Host-Namen in IP-Nummern erlaubt und andere Domänen-Informationen enthält.
Echtzeitblockliste	Onlinedatenbanken mit Spam-IP-Adressen Eingehende E-Mails werden mit dieser Liste abgeglichen um zu erkennen, ob sie von Benutzern stammen, die auf einer Blockliste stehen.
E-Mail-Überwachungsregeln	Regeln, die die Replikation der E-Mails zwischen E-Mail-Adressen erlauben.
Falsch-negative Ergebnisse	Spam-E-Mails, die nicht als Spam erkannt werden.
Falsch-positive Ergebnisse	Zulässige E-Mails, die fälschlicherweise als Spam erkannt werden.
Greylist-Filterung	Ein Anti-Spam-Filter, der E-Mails von Spammern blockiert, die keine Nachricht zurückschicken, wenn eine Versuchsnachricht empfangen wurde.
Haftungsausschluss	Eine Erklärung, die den Umfang der Rechte und Pflichten von E-Mail-Empfängern begrenzt oder definiert.
Ham	Zulässige E-Mail
IIS	*Siehe* Internet-Informationsdienste
IMAP	*Siehe* Internet Message Access Protocol
Intelligenter Hintergrund-Übertragungsdienst	Eine Komponente des Windows-Betriebssystems, die die Übertragung von Dateien zwischen Systemen unter Nutzung der leeren Netzwerkbandbreite unterstützt.

Internet Message Access Protocol	Eines der beiden am häufigsten verwendeten Internetstandardprotokolle zum Laden von E-Mails, das andere ist POP3.
Internetinformationsdienste	Eine Reihe von Internetdiensten der Microsoft Corporation für Internetserver
LDAP	*Siehe* Lightweight Directory Access Protocol
Lightweight Directory Access-Protokoll	Ein Anwendungsprotokoll zur Abfrage und Bearbeitung von Verzeichnisdiensten unter TCP/IP
Listenserver	Ein Server, der E-Mails an Diskussionslisten und Newsletter-Listen verteilt und Abonnementanfragen verwaltet.
Mail Exchange	Der DNS-Eintrag für die Identifizierung der IP-Adressen der Domänen-Mailserver.
MAPI	*Siehe* Messaging Application Programming Interface
MDAC	*Siehe* Microsoft Data Access Components.
Messaging Application Programming Interface	Eine Nachrichtenarchitektur und eine auf dem Komponenten-Objektmodell basierende Anwendungsprogrammierschnittstelle für Microsoft Windows.
Microsoft Data Access Components	Eine Windows-Technologie, mit der Entwickler eine homogene und konsistente Möglichkeit zur Entwicklung von Software erhalten, die auf fast jeden Datenspeicher zugreifen kann.
Microsoft Message Queuing Services	Eine Implementierung einer Warteschlange für Windows-Server-Betriebssysteme.
MIME	*Siehe* Multipurpose Internet Mail Extensions
MSMQ	*Siehe* Microsoft Message Queuing Services
Multipurpose Internet Mail Extensions	Ein Standard, der das Format von E-Mail so erweitert, dass nicht nur ASCII-Text unterstützt wird, sondern auch anderer Text, Anhänge, die kein Text sind, Nachrichtentexte mit mehreren Teilen und Header-Daten mit anderen als ASCII-Zeichensätzen.
NDR	*Siehe* Unzustellbarkeitsbericht.
Öffentlicher Order	Ein gemeinsamer Ordner, mit dem Microsoft Exchange-Benutzer Informationen austauschen können.
Perimeter Server/Gateway	Der Computer (Server) in einem Netzwerk, der direkt mit einem externen Netzwerk verbunden ist. In GFI MailEssentials bezieht sich der Begriff Perimeter Gateway auf die E-Mail-Server im Unternehmen, die E-Mails direkt von externen Domänen erhalten.
Phishing	Die Sammlung sensitiver persönlicher Daten mit Betrugsabsicht in der Regel mit Hilfe gefälschter Nachrichten.
POP2Exchange	Ein System, das E-Mail-Nachrichten von POP3-Mailboxen holt und an den E-Mail-Server weiterleitet.
POP3	*Siehe* Post Office Protocol ver.3
Post Office Protocol ver.3	Ein Protokoll für lokale E-Mail-Clients um E-Mails aus Postfächern über eine TCP/IP-Verbindung zu laden.
Quarantäne	Eine Datenbank, wo alle als Spam erkannten, eingehenden E-Mails für einige Tage verbleiben.
RBL	*Siehe* Echtzeitblockliste.
Remote-Befehle	Anweisungen, die es erlauben, Aufgaben aus der Ferne auszuführen.
Secure Sockets Layer	Ein Protokoll, das die sichere und ganzheitliche Kommunikation zwischen Netzwerken gewährleistet.

Simple Mail Transfer-Protokoll	Ein Internetstandard für die E-Mail-Übertragung zwischen IP-Netzwerken.
SMTP	*Siehe* Simple Mail Transport Protocol.
Spam-Aktionen	Aktionen für eingegangene Spam-Mails, beispielsweise das Löschen der Spam-Mails oder Versand in einen Junk-Ordner.
SSL	*Siehe* Secure Sockets Layer.
Unzustellbarkeitsbericht	Eine automatische E-Mail-Nachricht, die den Absender informiert, dass eine E-Mail nicht zugestellt werden konnte.
WebDAV	Eine HTTP-Erweiterungsdatenbank, mit der Benutzer Dateien aus der Ferne interaktiv verwalten können. Zur Verwaltung von E-Mails in dem Postfach und dem öffentlichen Ordner in Microsoft Exchange.
Whitelist	Eine Liste der E-Mail-Adressen und Domänen, von denen laufend E-Mails eingehen.
Zombie	Ein infizierter Computer, der Teil eines Botnets ist.

2 Informationen zu GFI MailEssentials

2.1 Mindestanforderungen und Installation

Informationen zu Systemanforderungen und zur Installation finden Sie in der 'Kurzanleitung für GFI MailEssentials'.

http://www.gfi.com/mes/manual

2.2 Wie funktionieren Spam-Filter?

2.2.1 Filtern eingehender E-Mails

Das Filtern eingehender E-Mails ist ein Vorgang, bei dem eingehende E-Mails vor der Zustellung an die Benutzer analysiert werden.

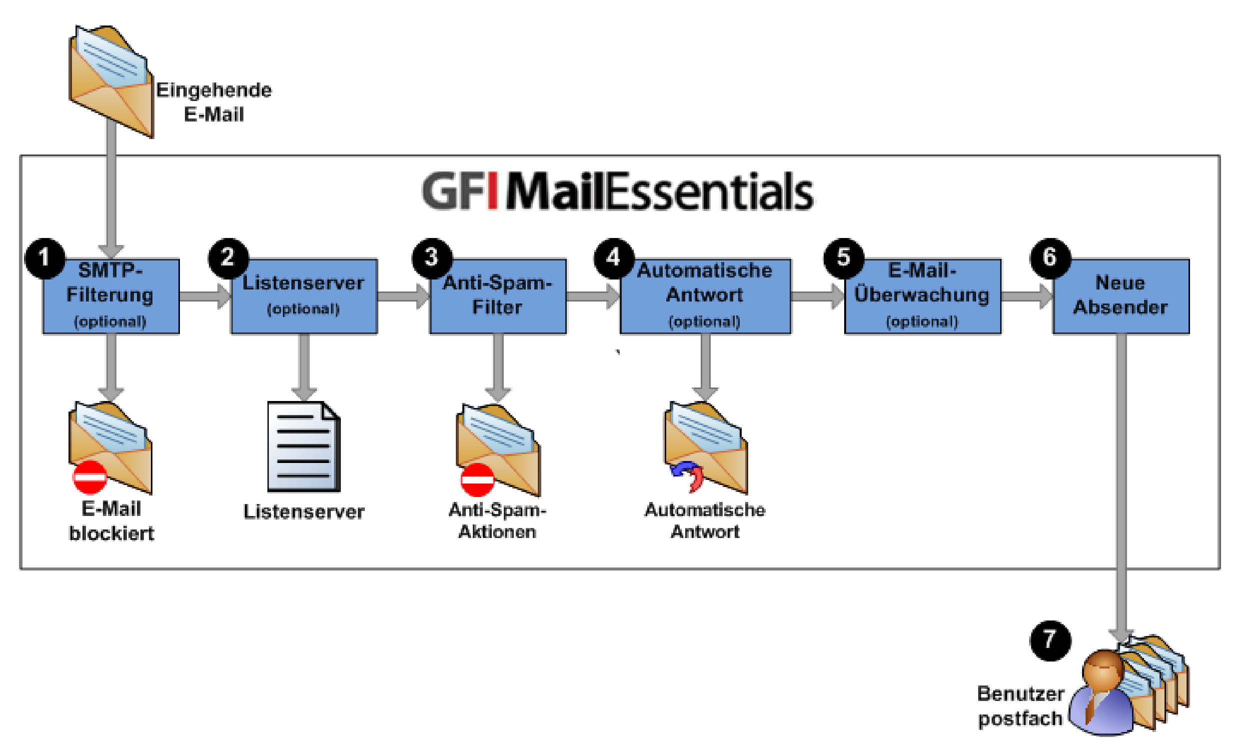


Abbildung 1 - Filtern eingehender E-Mails

Bei Empfang einer E-Mail:

❶ Die Filterung auf SMTP-Ebene (Directory Harvesting und Greylist) wird ausgeführt, bevor der E-Mail-Text empfangen wird.

❷ Es wird geprüft, ob die E-Mail an eine Liste im Listenserver adressiert ist. Wenn die E-Mail zu einer Liste gehört, wird sie vom Listenserver verarbeitet.

❸ Die eingehende E-Mail wird durch alle Spam-Filter gefiltert. Jede E-Mail, die die Spam-Filterprüfung nicht besteht, wird mit den für Spam-Mails definierten Aktionen weiter bearbeitet. Wenn eine E-Mail alle Spam-Filter passiert und nicht als Spam identifiziert wird, erfolgt die nächste Stufe der Prüfung.

❹ Bei entsprechender Konfiguration werden automatische Antworten an den Absender gesendet.

❺ Bei entsprechender Konfiguration wird die E-Mail-Überwachung ausgeführt und es werden die entsprechenden Maßnahmen ergriffen.

❻ Der Filter "Neue Absender" wird ausgeführt.

❼ Die E-Mail wird in das Benutzerpostfach gesendet.

2.2.2 Filtern ausgehender E-Mails

Das Filtern ausgehender E-Mails ist ein Vorgang, bei dem von den Benutzern versendete E-Mails im Unternehmen verarbeitet und dann erst abgesendet werden.

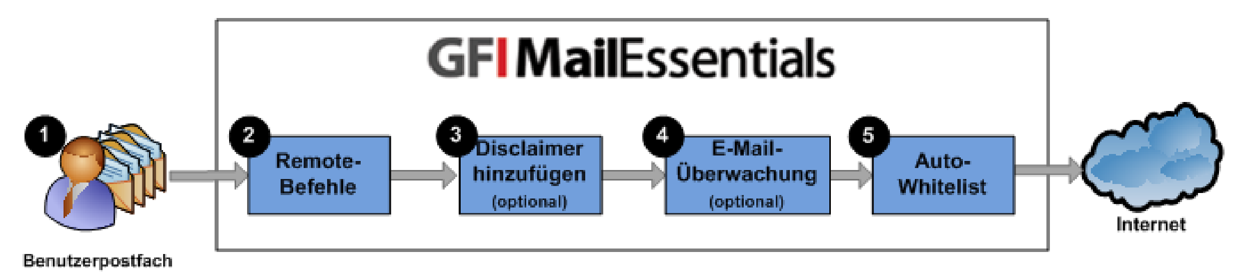


Abbildung 2 - Filtern ausgehender E-Mails

❶ Der Benutzer erstellt und versendet E-Mails.

❷ Die Funktion für Remote-Befehle sucht nach Remote-Befehlen in E-Mails und führt diese aus. Wenn keine gefunden werden, wird die E-Mail in der nächsten Stufe weiterverarbeitet.

❸ Bei entsprechender Konfiguration wird ein definierter Haftungsausschluss in der E-Mail ergänzt.

❹ Es wird für die E-Mail überprüft, ob eine E-Mail-Überwachung eingerichtet ist, und es werden entsprechend den gegebenenfalls konfigurierten Regeln Aktionen ausgeführt.

❺ Falls Auto-Whitelist aktiviert ist, wird der Empfänger der E-Mail-Adresse der Whitelist hinzugefügt. Dadurch werden automatisch die Antworten diese Empfängers an den Absender geleitet, ohne dass auf Spam geprüft wird. Nach dieser Prüfung wird die E-Mail an den Empfänger geschickt.

2.3 Beschreibung der Anti-Spam-Filter und Aktionen

Informationen über Spam-Filter

GFI MailEssentials enthält standardmäßig bereits eine Reihe spezieller Spam-Filter. Jeder einzelne dieser Filter ist für eine bestimmte Art von Spam-Mails gedacht. Zusammen mit GFI MailEssentials werden folgende Filter ausgeliefert:

FILTER	BESCHREIBUNG	STANDARD-MÄßIG AKTIVIERT
SpamRazer	Ein Spam-Filter, der erkennt, ob eine E-Mail Spam ist. Dazu wird die E-Mail-Herkunft, der Inhalt der Nachricht und deren Transportweg analysiert.	Ja
Directory Harvesting	Das Modul stoppt E-Mails, die nach dem Zufallsprinzip erzeugt an einen Server gesendet werden, für die aber meist keine Benutzer existieren.	Nein
Phishing	Dieser Filter blockiert E-Mails, die Links in den Nachrichtentexten enthalten, die auf bekannte Phishing-Sites zeigen oder typische Phishing-Keywords enthalten.	Ja
Sender Policy Framework	Dieser Filter stoppt E-Mails, die von Domänen stammen, die in den SPF-Records nicht autorisiert wurden.	Nein
Auto-Whitelist	Wenn an diese Adressen eine E-Mail gesendet wird, werden Spam-Filter automatisch ignoriert.	Ja
Whitelists	Eine benutzerdefinierte Liste sicherer E-Mail-Adressen	Ja
E-Mail-Blocklist	Eine benutzerdefinierte Liste gesperrter E-Mail-Nutzer oder Domänen.	Ja

Filter	Beschreibung	Standard-mäßig aktiviert
IP-DNS-Blocklist	Prüft, ob die empfangene E-Mail von Absendern stammt, die in einer öffentlichen DNS-Blockliste bekannter Spammer enthalten sind.	Ja
URI-DNS-Blocklist	Dieser Filter stoppt E-Mails, die Links zu Domänen enthalten, die in den öffentlichen Spam-URL-Blocklists enthalten sind, beispielsweise sc.surbl.org.	Ja
Header-Prufüng	Dieses Modul analysiert die einzelnen Felder im Header durch Vergleich mit dem SMTP- und MIME-Feld.	Ja
Keyword-Prufüng	Spam-Mails werden anhand gesperrter Keywords in der E-Mail-Überschrift oder in der E-Mail-Nachricht identifiziert.	Nein
Neue Absender	E-Mails, die von Absendern stammen, an die noch nie eine E-Mail gesendet wurde.	Nein
Bayes'sche Analyse	Ein Spamverfahren, bei dem nach Training durch die Benutzer Spam-Mails mit statistischen Verfahren identifiziert werden.	Nein
Greylist	Erkennt E-Mails von nicht RFC-konformen Mailservern, die normalerweise von Spammern verwendet werden.	Nein

Wie aus der Tabelle oben zu ersehen, sind nicht alle Spam-Filter standardmäßig aktiviert. Dies hängt damit zusammen, dass die Konfigurationseinstellungen netzwerk- und infrastrukturabhängig sind und daher nicht voreingestellt werden können. Obgleich wichtige Filter wie SpamRazer standardmäßig aktiviert sind, sollten Sie nach der Installation von GFI MailEssentials die übrigen Spam-Filter und Filtermechanismen prüfen und aktivieren. Weitere Informationen finden Sie unter **Spam-Filter** in diesem Handbuch.

Spam-Aktionen

Bei der Erkennung einer Spam-E-Mail können die Anti-Spam-Filter verschiedene Aktionen auslösen. Diese Aktionen bestimmen, was mit der als Spam erkannten E-Mail geschieht, und sind auf einer Filter-zu-Filter-Basis konfigurierbar. Unterstützte Anti-Spam-Filteraktionen sind:

- Spam löschen,
- E-Mail-Aufbewahrung in Quarantäne (empfohlene Aktion),
- Verschieben von Spam-E-Mails in ein Postfach,
- Weiterleiten von Spam-E-Mails an eine bestimmte E-Mail-Adresse,
- Speichern von Spam-E-Mails in einem Ordner auf einem Datenträger,
- Kennzeichnen von Spam-E-Mails,
- Verschieben von Spam-E-Mails in einen zentralen Ordner,
- Weiterleiten von Spam-E-Mails an öffentliche E-Mail-Ordner,

Weitere Informationen zu Anti-Spam-Aktionen finden Sie im Abschnitt **Spam-Aktionen - Umgang mit Spam-Mails** in diesem Handbuch.

Standardmäßige Anti-Spam-Aktionen

Die von GFI MailEssentials durchgeführte Aktion zur Blockierung von Spam-E-Mails kann im Nachinstallationsassistent festgelegt werden. Falls der Nachinstallationsassistent übersprungen wird, hängt die von GFI MailEssentials durchgeführte Aktion zur Blockierung von Spam-E-Mails vom Installationsort der Software ab:

Installation	Standardmaßnahme	Beschreibung
GFI MailEssentials ist auf	E-Mail wird in den	Wenn ein Filter eine Spam-E-Mail

INSTALLATION	STANDARDMAßNAHME	BESCHREIBUNG
demselben Computer wie Microsoft Exchange installiert.	Unterordner des Exchange-Postfachs verschoben.	blockiert, wird die E-Mail in einen Unterordner im Posteingang mit der Bezeichnung „Vermutliche Spam“ verschoben.
GFI MailEssentials ist nicht auf demselben Rechner wie Microsoft Exchange installiert.	Kennzeichnung	Spamfilter ergänzt Präfix [SPAM] im Betreff-Feld der E-Mails. Gekennzeichnete E-Mails werden immer noch in den Posteingang des Benutzers geleitet.

Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt **Spam-Aktionen - Umgang mit Spam-Mails** in diesem Handbuch.

2.4 Registrierung

Informationen zur Registrierung erhalten Sie hier:

http://www.gfi.com/products/gfi-mailessentials/pricing/licensing

3 Anzeigen des Anti-Spam-Verarbeitungsstatus

3.1 Verwenden des Dashboards von GFI MailEssentials

Im Dashboard von GFI MailEssentials wird der Status des Anti-Spam-Systems einschließlich der Verarbeitung und Statistiken für E-Mails angezeigt.

3.1.1 Überwachen des Status in Echtzeit

Im Dashboard von GFI MailEssentials können Sie die Dienste und die E-Mail-Verarbeitung von GFI MailEssentials in Echtzeit überwachen.

1. Klicken Sie auf **Start** ▶ **Alle Programme** ▶ **GFI MailEssentials** ▶ **GFI MailEssentials Dashboard**.

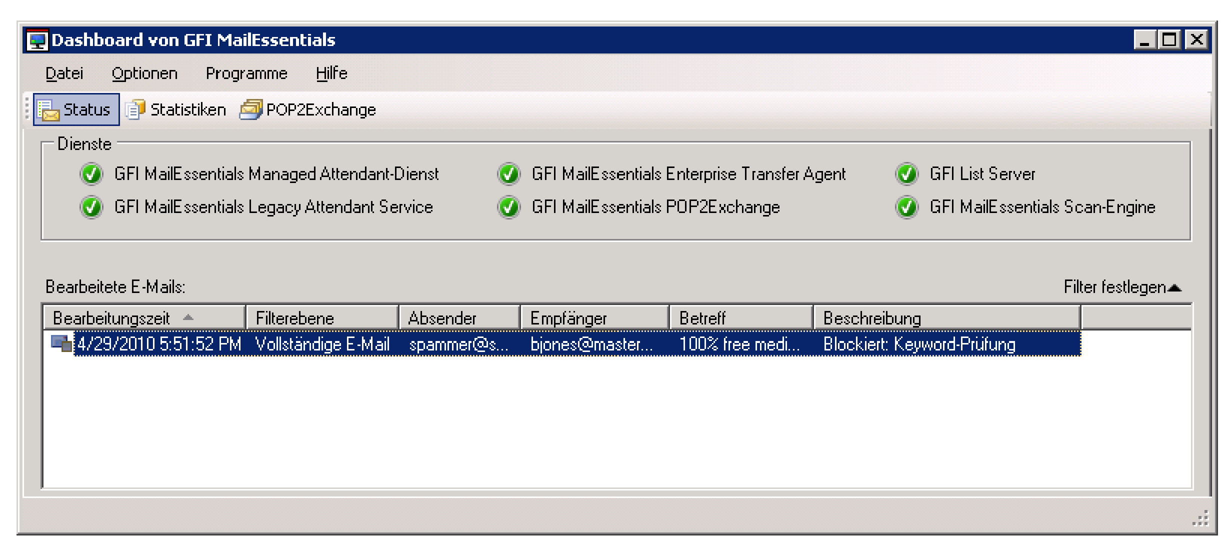


Abbildung 1 - GFI MailEssentials-Dashboard: Registerkarte „Status"

2. Wählen Sie die Registerkarte **Status** aus.

Im Bereich **Dienste** wird der Status der Dienste von GFI MailEssentials angezeigt. Damit die Software ordnungsgemäß funktioniert, müssen alle Dienste aktiviert sein.

Der Bereich **Bearbeitete E-Mails** enthält die von GFI MailEssentials bearbeiteten E-Mails sowie eine Beschreibung des E-Mail-Status. Sie können die Liste der bearbeiteten E-Mails auch filtern. Klicken Sie dazu auf **Filter anzeigen**. Geben Sie die gewünschten Filterkriterien ein. Übereinstimmungen werden in der Liste angezeigt. Sie können folgende Filterkriterien verwenden:

- Betreff
- Nachrichten-ID
- Absender
- Empfänger

Darüber hinaus kann die Liste noch nach Typ und Beschreibung der E-Mail gefiltert werden. Navigieren Sie zu **Optionen** ▶ **E-Mail-Protokollfilter**, und treffen Sie eine Auswahl, um E-Mails anzuzeigen, die folgenden Kriterien entsprechen:

- **Gesendete E-Mail** - Diese Nachrichten konnten den vorgesehenen Empfängern zugestellt werden.
- **E-Mail blockiert** - Diese Nachrichten wurden von einem Anti-Spam-Filter blockiert.
- **Whitelist-E-Mail** - Diese Nachrichten weisen einen entsprechenden Whitelist-Eintrag auf und wurden den vorgesehenen Empfängern ohne weitere Prüfung zugestellt.

- **E-Mail-Fehler** - Diese Nachrichten konnten nicht gescannt oder zugestellt werden. Die Nachrichten werden im Ordner **FailedMails** im Installationsordner von GFI MailEssentials gespeichert.
- **Eingehende E-Mails** - Diese eingehenden Nachrichten sind an lokale Benutzer adressiert.
- **Ausgehende E-Mails** - Diese ausgehenden Nachrichten wurden von lokalen Benutzern an externe Benutzer gesendet.

HINWEIS: Navigieren Sie zu **Optionen** ► **Spalten auswählen**, um die Spalten auszuwählen, die in der Liste der bearbeiteten E-Mails angezeigt werden sollen.

3.1.2 Statistik

Auf der Registerkarte „Statistik“ des Dashboards von GFI MailEssentials können Sie statistische Informationen zum Scannen von E-Mails anzeigen.

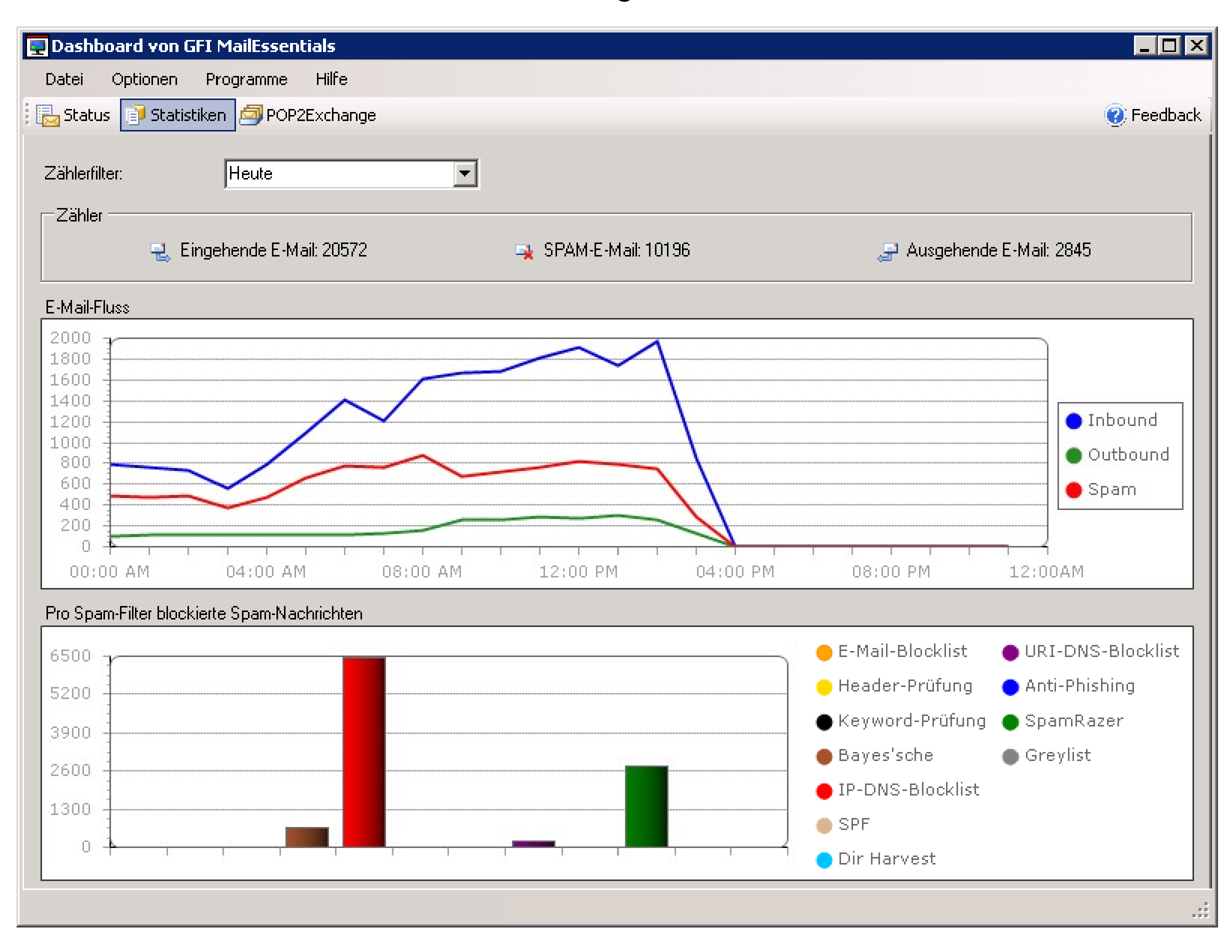


Abbildung 2 - GFI MailEssentials-Dashboard: Registerkarte Statistik

- **Zählerfilter** - Legt den Zeitraum für die anzuzeigende Statistik fest.
- **Zähler** - Zeigt die Anzahl der ein- und ausgehenden E-Mails sowie die Anzahl der E-Mails an, die als Spam identifiziert wurden.
- **E-Mail-Fluss** - Dieses Zeitdiagramm zeigt, je nachdem welcher Zeitraum ausgewählt wird, die Anzahl der eingehenden, ausgehenden und als Spam eingestuften E-Mails an, die pro Stunde oder pro Tag verarbeitet wurden.
- **Pro Spam-Filter blockierte Spam-Nachrichten** - Zeigt die Anzahl der E-Mails an, die von jedem Spam-Filter blockiert wurden.

3.1.3 POP2Exchange

Auf der Registerkarte „POP2Exchange“ des Dashboards von GFI MailEssentials wird ein Protokoll der Aktivitäten von POP2Exchange angezeigt.

HINWEIS: Informationen zu POP2Exchange finden Sie unter **Konfiguration von POP3 und**

Download-Einwahlverbindung in diesem Handbuch.

3.2 Erzeugen von Spam-Berichten

Der Spam-Bericht ist ein Kurzbericht, der dem Benutzer oder Administrator per E-Mail gesendet wird. Dieser Bericht führt die Gesamtzahl der von GFI MailEssentials verarbeiteten E-Mails sowie die Zahl der geblockten Spam-Mails innerhalb eines bestimmten Zeitraums auf (… in der Regel seit dem letzten Spam-Bericht).

3.2.1 Konfigurieren von Spam-Berichten

Administrator-Spam-Bericht

1. Klicken Sie auf **Anti-Spam** ► **Spam-Bericht** ► **Eigenschaften**.

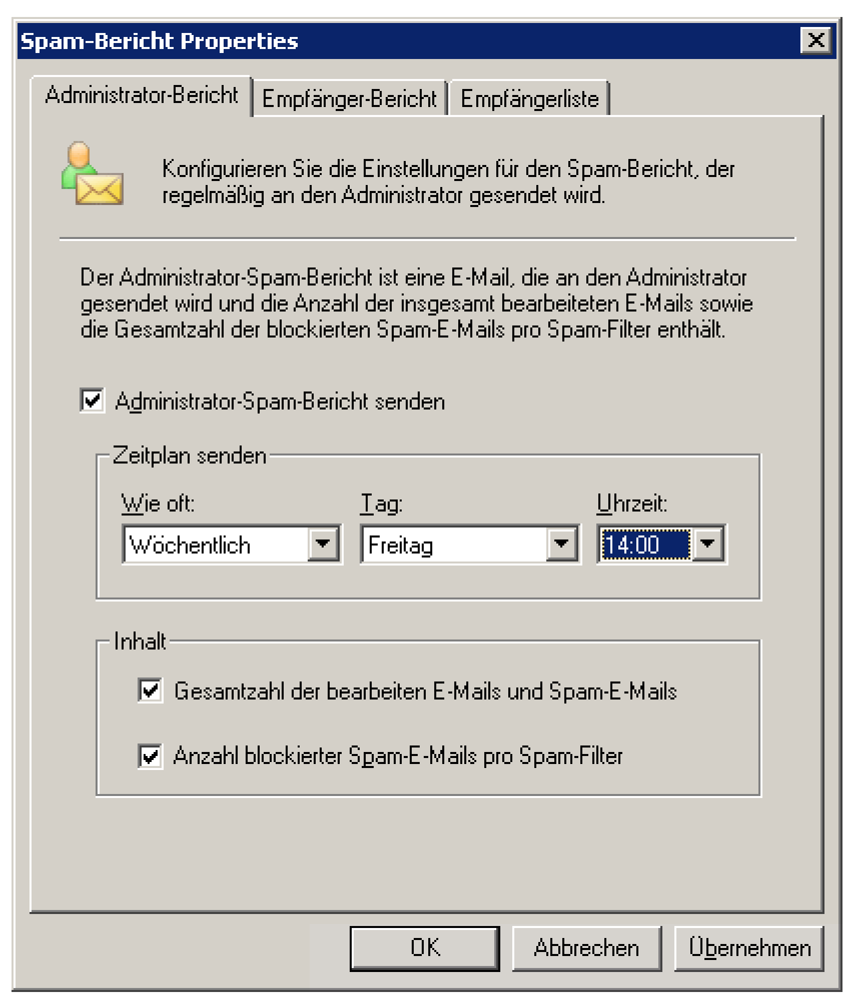


Bild 3 - Spam-Bericht-Eigenschaften/Administrator-Spam-Bericht

2. Klicken Sie auf der Registerkarte **Administrator-Bericht** auf **Administrator-Spam-Bericht senden** um den Spam-Bericht zu aktivieren.

3. Konfigurieren Sie die gewünschte Sendehäufigkeit (täglich, wöchentlich, monatlich) über die Dropdown-Liste **Sendezeitplan**.

4. Geben Sie an, welchen Inhalt der Spam-Bericht in der E-Mail haben soll, entweder die **Gesamtzahl der verarbeiteten E-Mails und Spam-Mails** oder die **Gesamtzahl der pro Spam-Filter geblockten Spam-Mails** oder beide Angaben.

5. Schließen Sie die Einstellungen ab, indem Sie auf **Übernehmen** und **OK** klicken.

Empfänger-Spam-Bericht

1. Klicken Sie auf **Anti-Spam** ► **Spam-Bericht** ► **Eigenschaften**.

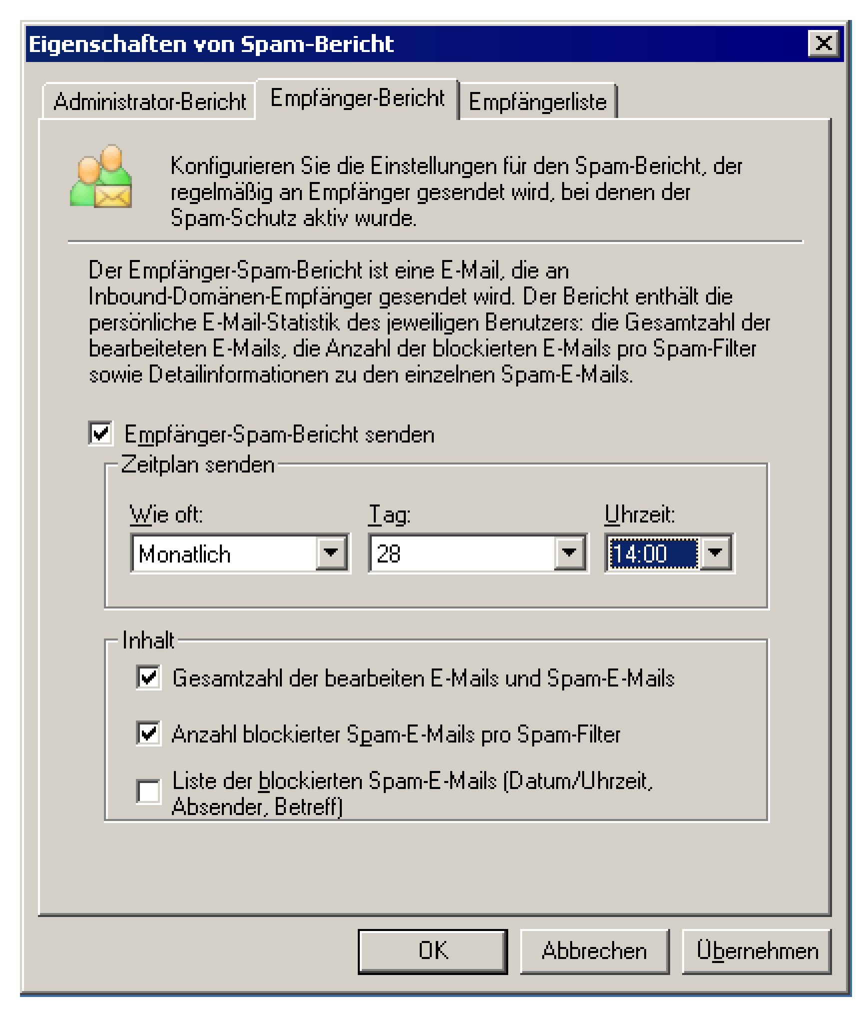


Bild 4 - Empfänger-Spam-Bericht

2. Klicken Sie auf der Registerkarte **Empfänger-Bericht** auf die Option **Empfänger Spam-Bericht senden** um einen Spam-Bericht zu aktivieren.

3. Konfigurieren Sie die gewünschte Sendehäufigkeit über die Option **Sendezeitplan**.

4. Legen Sie fest, was in dem in der E-Mail gesendeten Bericht enthalten sein soll:

» Gesamtzahl der verarbeiteten E-Mails und Spam-Mails

» Gesamtzahl der pro Spam-Filter geblockten Spam-Mails

» Liste der geblockten Spam-Mails

Oder eine beliebige Kombination dieser Optionen, je nach Bedarf.

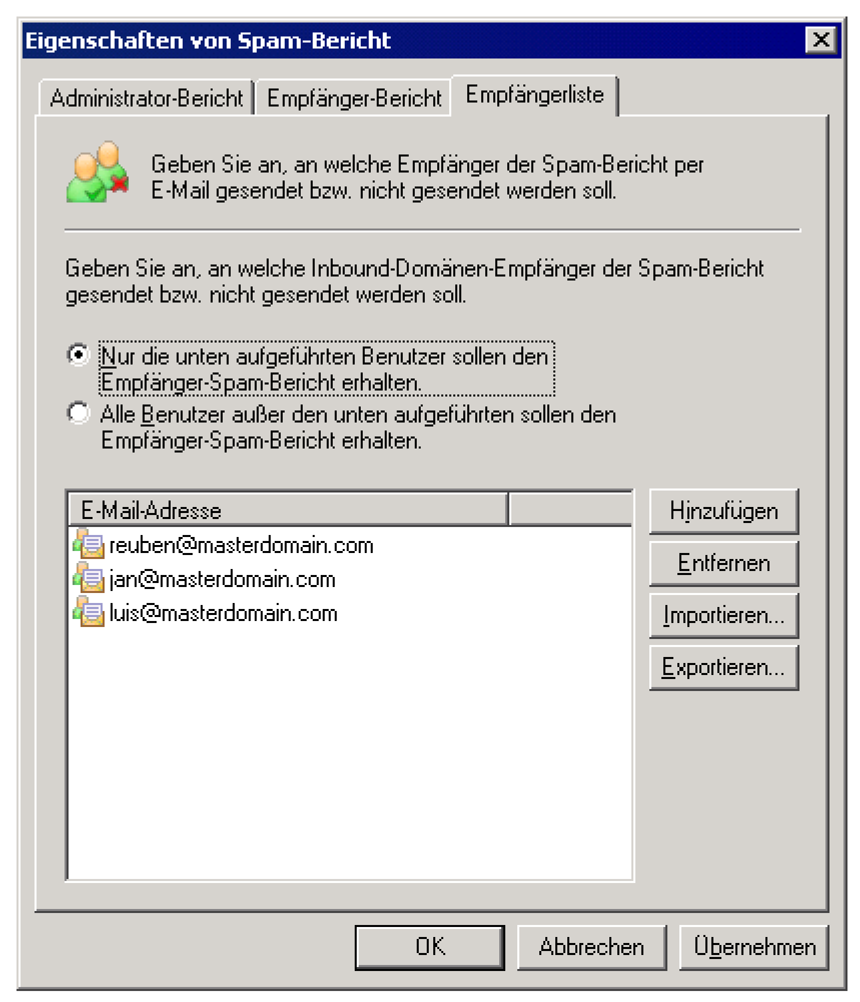


Bild 5 - Spam-Bericht-Empfängerliste

5. Klicken Sie auf die Registerkarte **Empfänger**, ergänzen Sie die Benutzer, die den Spam-Bericht erhalten sollen und wählen Sie aus, wie entschieden werden soll, wer den Spam-Bericht empfängt. Verfügbare Optionen:

» Nur die im Folgenden aufgelisteten Benutzer sollten einen Empfänger-Spam-Bericht erhalten.

» Alle Nutzer außer den im Folgenden aufgelisteten Benutzern erhalten den Empfänger-Spam-Bericht.

HINWEIS: Die benötigte Benutzerliste kann auch aus einer Datei im XML-Format importiert werden, wenn diese die gleiche Struktur besitzt, mit der GFI MailEssentials Daten exportiert.

6. Klicken Sie auf **Übernehmen** und **OK** um die Einstellungen abzuschließen.

3.3 Berichte zur E-Mail-Verarbeitung und zum Spam-Status

GFI MailEssentials erlaubt die Erstellung von Berichten über in der Datenbank archivierte Daten. Mit Hilfe dieser Berichte erkennen Sie, welche Spam-Mails von GFI MailEssentials ausgefiltert werden und wie Ihre Domänenressourcen und Ihr Mailserver ausgelastet sind.

3.3.1 Aktivieren von Berichten

1. Klicken Sie auf **E-Mail-Verwaltung** ► **Berichterstellung** ► **Eigenschaften** und anschließend auf die Schaltfläche **Konfigurieren**.

2. Wählen Sie dann den Datenbanktyp aus:

» **Microsoft Access** - Geben Sie Dateiname und Standort an.

» **Microsoft SQL Server** - Geben Sie Servername, Authentifizierungsdaten und Datenbank an.

3. Klicken Sie auf die Schaltfläche **Testen** um die Datenbankkonfiguration zu testen. Klicken Sie auf **OK** um die Einstellung zu speichern.

Konfigurieren der automatischen Datenbankbereinigung

Sie können GFI MailEssentials auch so konfigurieren, dass Einträge in der Datenbank, die ein bestimmtes Alter erreicht haben, automatisch gelöscht (bereinigt) werden. So aktivieren Sie die automatische Bereinigung:

1. Navigieren Sie zu **E-Mail-Verwaltung ► Berichterstellung ► Eigenschaften**, und wählen Sie die Registerkarte **Automatische Bereinigung** aus.

2. Wählen Sie **Einträge bereinigen, die älter sind als** aus, und geben Sie den Zeitraum für die automatische Bereinigung in Monaten an.

HINWEIS: Die automatische Bereinigung wird nur auf die aktuelle Datenbank angewendet, die auf der Registerkarte **Berichterstellung** konfiguriert wurde.

3. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

3.3.2 Verwendung von Berichten

1. Starten Sie die Berichterstattung von GFI MailEssentials, indem Sie auf **Start ► Alle Programme ► GFI MailEssentials ► GFI MailEssentials-Berichte** klicken.

2. Klicken Sie auf die Option **Berichte** und wählen Sie dann einen Bericht /eine Statistik auf der Seite Statistik aus.

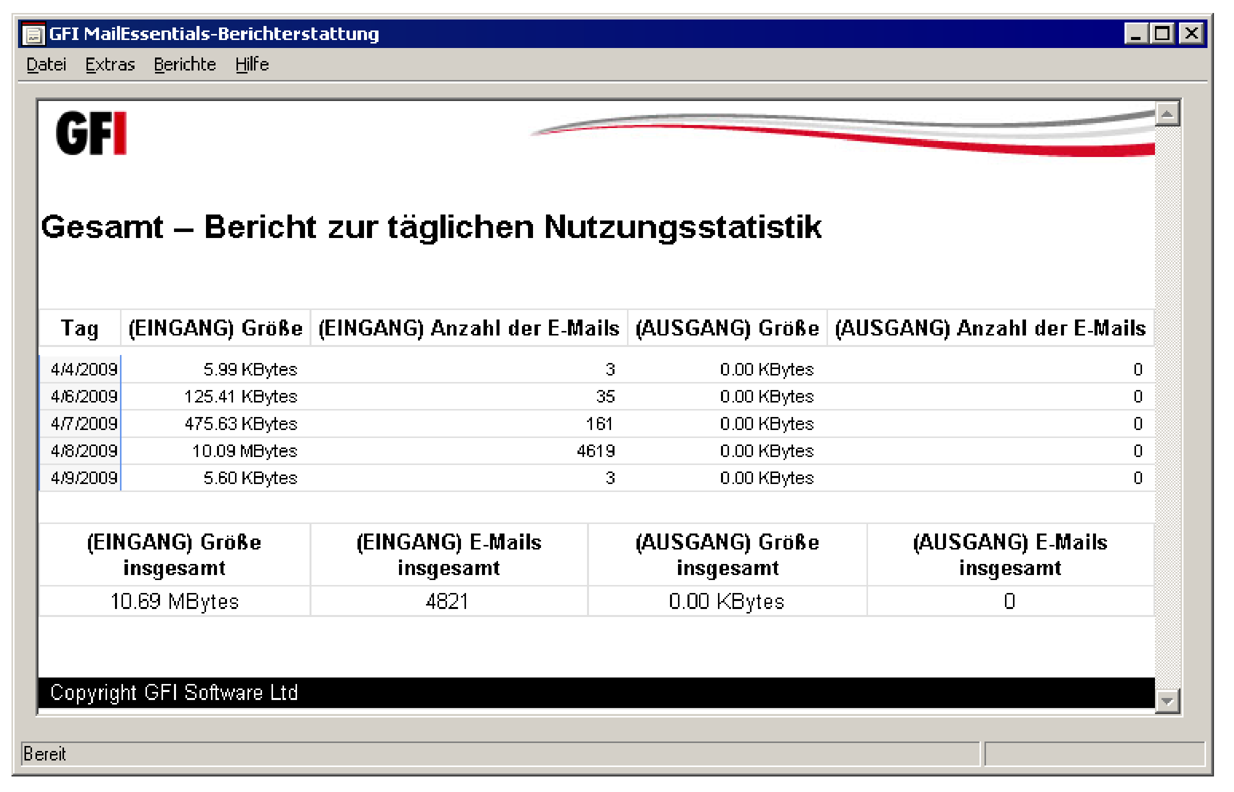
3. Legen Sie die Berichtskriterien fest, und klicken Sie auf **Bericht**, um den Bericht zu generieren.

4. Berichte können im HTML-Format gespeichert oder ausgedruckt werden.

HINWEIS: Beim Speichern des Berichts im HTML-Format werden die beiden Unterordner „Graphics“ und „Report“ erstellt. Im Unterverzeichnis „Report“ werden die Berichtdateien im HTML-Format abgelegt. Im Unterverzeichnis „Graphics“ werden alle Grafiken abgelegt, die im HTML-Bericht angezeigt werden.

Täglicher Spam-Bericht

Der tägliche Spam-Bericht zeigt die Gesamtzahl der verarbeiteten E-Mails, die Gesamtzahl der erkannten Spam-Mails, den prozentualen Anteil der Spam-Mails an allen Mails und wie viele Spam-Mails durch jedes einzelne Spam-Funktion erkannt wurden. Jede Zeile in dem Bericht entspricht einem Tag.



Gesamt – Bericht zur täglichen Nutzungsstatistik

Tag	(EINGANG) Größe	(EINGANG) Anzahl der E-Mails	(AUSGANG) Größe	(AUSGANG) Anzahl der E-Mails
4/4/2009	5.99 KBytes	3	0.00 KBytes	0
4/6/2009	125.41 KBytes	35	0.00 KBytes	0
4/7/2009	475.63 KBytes	161	0.00 KBytes	0
4/8/2009	10.09 MBytes	4619	0.00 KBytes	0
4/9/2009	5.60 KBytes	3	0.00 KBytes	0

(EINGANG) Größe insgesamt	(EINGANG) E-Mails insgesamt	(AUSGANG) Größe insgesamt	(AUSGANG) E-Mails insgesamt
10.69 MBytes	4821	0.00 KBytes	0

Copyright GFI Software Ltd

Bereit

Bild 6 - Täglicher Spam-Bericht

Berichtsoptionen

- **Spalte sortieren:** Sortieren Sie den Bericht nach Datum, Gesamtzahl der verarbeiteten Spams, Keyword-Prüfung usw.
- **Mehrseitiger Bericht:** Geben Sie an, wie viele Tage pro Seite angezeigt werden sollen.

Filteroptionen

- **Spezifische E-Mail:** Beschränken Sie den Bericht auf eine bestimmte E-Mail-Adresse.
- **Datumsbereich:** Beschränken Sie den Bericht auf einen bestimmten Datumsbereich.

Wenn Sie alle Berichtoptionen ausgewählt haben, klicken Sie auf **Bericht** um den Bericht zu erzeugen.

Anti-Spam-Regeln-Bericht

Der Bericht mit den Anti-Spam-Regeln zeigt, wie viele Spam-Mails mit jedem Spam-Filter erkannt wurden.

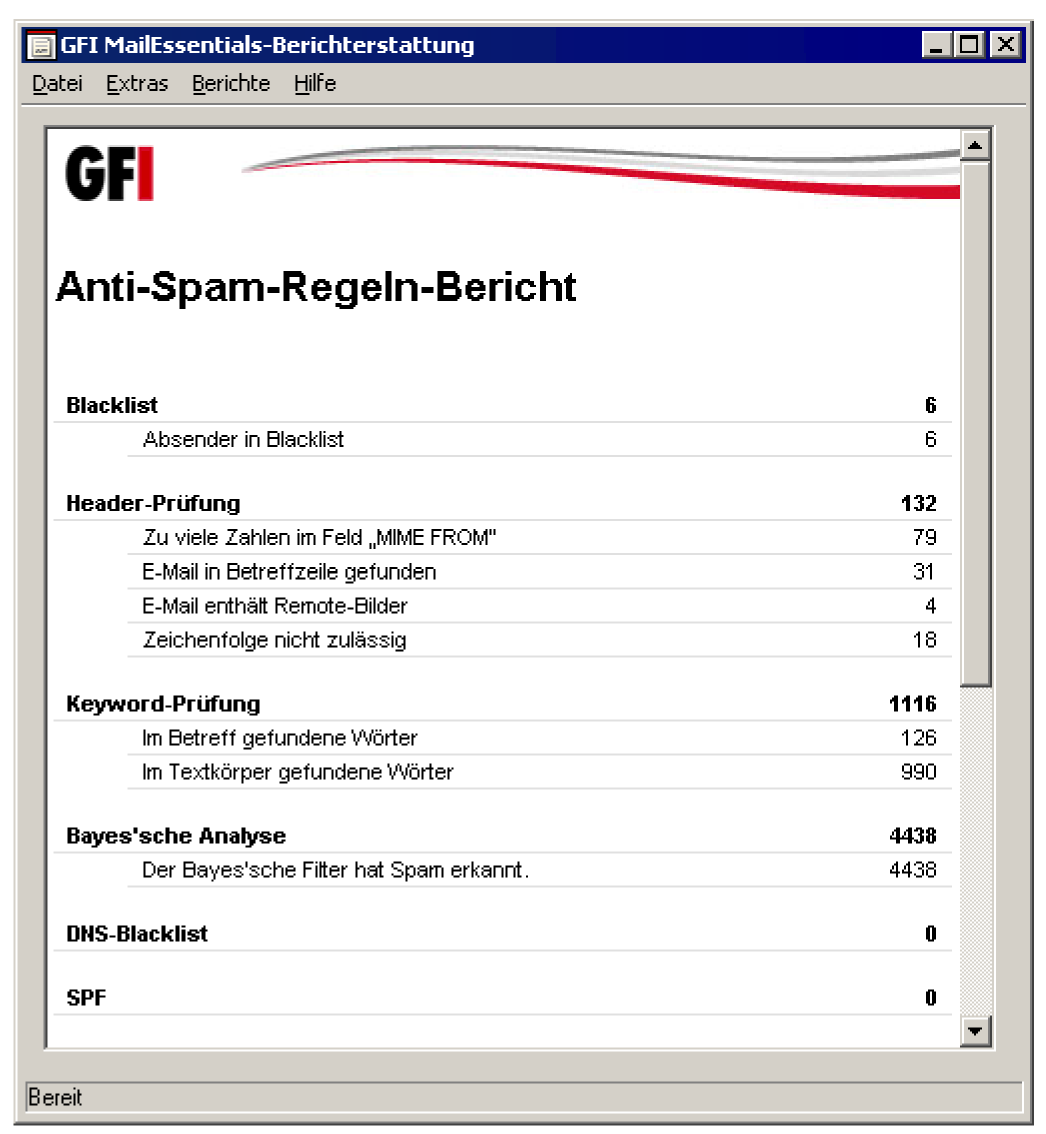


Bild 7 - Anti-Spam-Regeln-Bericht

Berichtsoptionen

- **Spezifische E-Mail:** Beschränkt den Bericht auf eine bestimmte E-Mail-Adresse.
- **Datumsbereich:** Beschränkt den Bericht auf einen bestimmten Datumsbereich.

Wenn alle Berichtsoptionen ausgewählt sind, klicken Sie auf die Schaltfläche **Bericht** um den Bericht zu erstellen.

Benutzer-Nutzungsstatistiken

Der Bericht mit den Benutzer-Nutzungsstatistiken zeigt in einer Übersicht, wie viele E-Mails die Benutzer versenden oder empfangen und wie groß die versendeten oder empfangenen E-Mails sind.

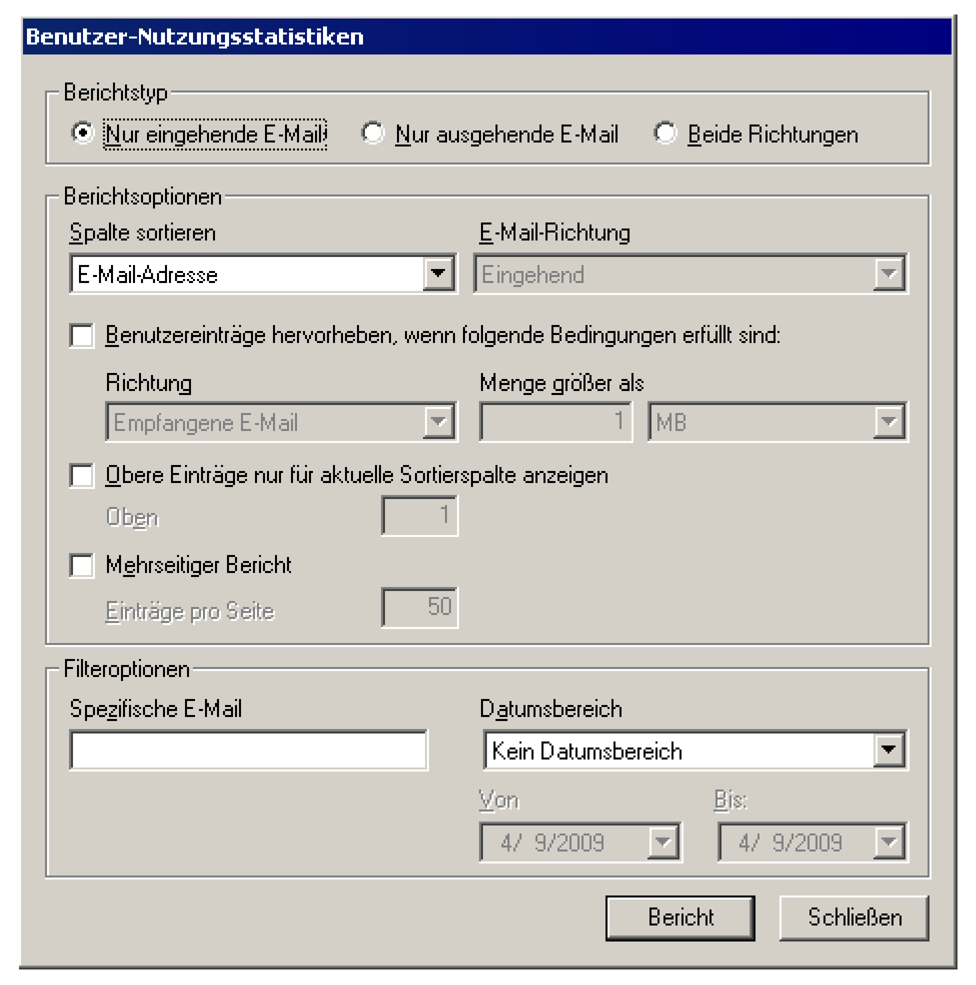


Bild 8 - Filterdialog "Benutzer-Nutzungsstatistik"

Berichtstyp

- **Berichtstyp:** Geben Sie an, ob Sie einen Bericht für die eingehenden E-Mails, die ausgehenden E-Mails oder beide erstellen wollen.

Berichtsoptionen

- **Sortierschlüssel:** Geben Sie an, ob die Sortierung nach E-Mail-Adresse, nach Anzahl der E-Mails oder nach der Gesamtgröße der E-Mails erfolgen soll.
- **Benutzer hervorheben:** Identifizieren Sie die Benutzer, die ungewöhnlich viele E-Mails oder ungewöhnlich große E-Mails empfangen oder versenden.
- **Nur wichtige anzeigen:** Zeigen Sie nur die wichtigsten Benutzer in dem Bericht an.
- **Mehrseitiger Bericht:** Geben Sie an, wie viele Benutzer pro Seite angezeigt werden sollen.

Filteroptionen

- **Spezifische E-Mail:** Beschränken Sie den Bericht auf eine bestimmte E-Mail-Adresse.
- **Datumsbereich**: Beschränkt den Bericht auf einen bestimmten Datumsbereich.

Wenn alle Berichtsoptionen ausgewählt sind, klicken Sie auf die Schaltfläche **Bericht** um den Bericht zu erstellen.

Domänen-Nutzungsstatistiken

Die Bericht mit der Domänen-Nutzungsstatistik zeigt in einer Übersicht, wie viele E-Mails an externe Domänen gesendet oder von dort empfangen wurden.

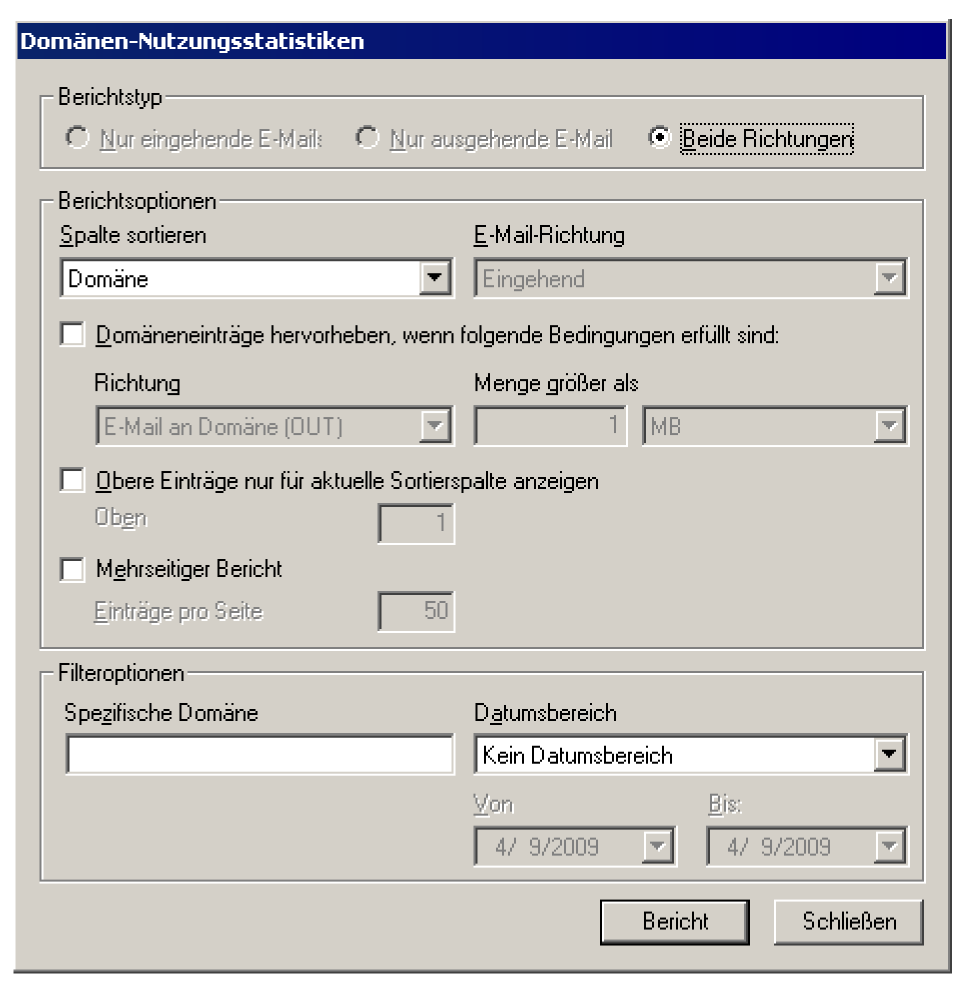


Bild 9 - Der Filterdialog "Domänen-Nutzungsstatistik"

Berichtstyp

» **Berichtstyp:** Standardmäßig enthält die Domänen-Nutzungsstatistik immer Daten für ausgehende und eingehende E-Mails.

Berichtsoptionen

» **Sortierschlüssel:** Geben Sie an, ob der Bericht nach Domänenname, nach Anzahl der E-Mails oder nach Gesamtgröße der E-Mails sortiert werden soll.

» **Domänen hervorheben:** Geben Sie die Domänen an, die eine ungewöhnlich große Zahl E-Mails oder ungewöhnlich große E-Mails empfangen oder versenden.

» **Nur wichtige anzeigen:** Zeigt nur die wichtigsten Domänen in dem Bericht an.

» **Mehrseitiger Bericht:** Geben Sie an, wie viele Domänen pro Seite angezeigt werden sollen.

Filteroptionen

» **Spezifische Domäne:** Beschränkt den Bericht auf eine bestimmte Domäne.

» **Datumsbereich:** Beschränkt den Bericht auf einen bestimmten Datumsbereich.

Wenn alle Berichtsoptionen ausgewählt sind, klicken Sie auf die Schaltfläche **Bericht** um den Bericht zu erstellen.

Tägliche E-Mail-Server-Nutzungsstatistiken

Dieser Bericht zeigt in einer Übersicht, wie viele E-Mails pro Tag von dem E-Mail-Server empfangen oder versendet werden, auf dem GFI MailEssentials installiert ist.

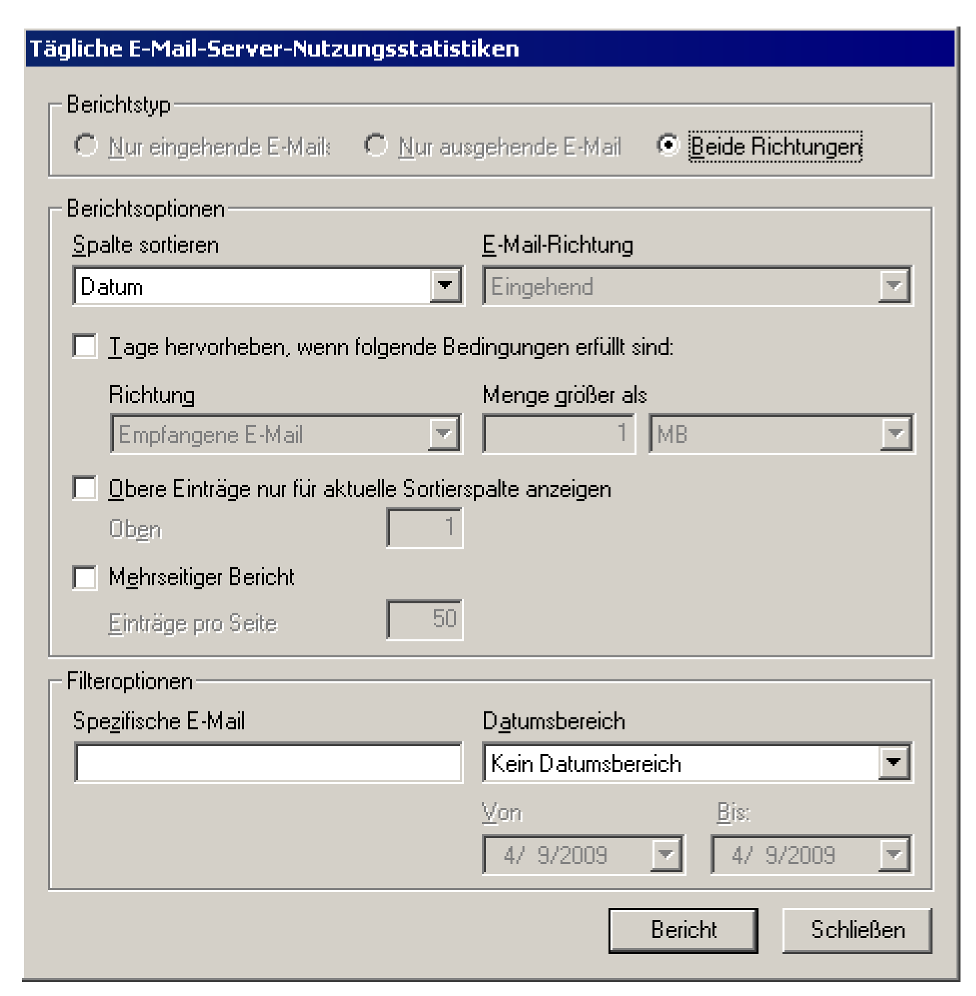


Bild 10 - Filterdialog "Tägliche E-Mail-Server-Nutzungsstatistik"

Berichtstyp

- **Berichtstyp:** Die Daten für die tägliche E-Mail-Server-Nutzungsstatistik werden immer für eingehende und ausgehende E-Mails angezeigt.

Berichtsoptionen

- **Sortierschlüssel:** Geben Sie an, ob der Bericht nach Datum sortiert werden soll (da der Bericht täglich erstellt wird), nach der Anzahl der E-Mails oder nach der Gesamtgröße der E-Mails.
- **Tage hervorheben:** Geben Sie die Tage an, an denen Sie mehr E-Mails oder größere E-Mails empfangen oder versendet haben als vordefiniert.
- **Nur wichtige anzeigen:** Zeigen Sie nur die wichtigsten definierten Tage in dem Bericht an.
- **Mehrseitiger Bericht:** Geben Sie an, wie viele Tage pro Seite angezeigt werden sollen.

Filteroptionen

- **Spezifische E-Mail:** Beschränkt den Bericht auf eine bestimmte Domäne.
- **Datumsbereich:** Beschränkt den Bericht auf einen bestimmten Datumsbereich.

Wenn alle Berichtsoptionen ausgewählt sind, klicken Sie auf die Schaltfläche **Bericht** um den Bericht zu erstellen.

Benutzerkommunikation

Der Bericht Benutzerkommunikation erlaubt Ihnen, zu kontrollieren, welche Art von E-Mails jeder Benutzer versendet hat. Wenn der Bericht zur Benutzerkommunikation einmal erstellt ist, kann der Benutzereintrag erweitert werden um den Betreff der gesendeten oder empfangenen E-Mails anzuzeigen. E-Mails mit dem gleichen Betreff werden in Gruppen zusammengefasst. Diese E-Mails können dann weiter analysiert werden um zu prüfen, wann und an wen die E-Mail mit

dem Betreff gesendet wurde.

Wichtige Hinweise

1. Dieser Bericht ist ein komplexer Bericht und seine Erstellung benötigt Zeit. Sie sollten den Umfang des Berichts auf einen bestimmten Benutzer oder einen bestimmten Datumsbereich einschränken.

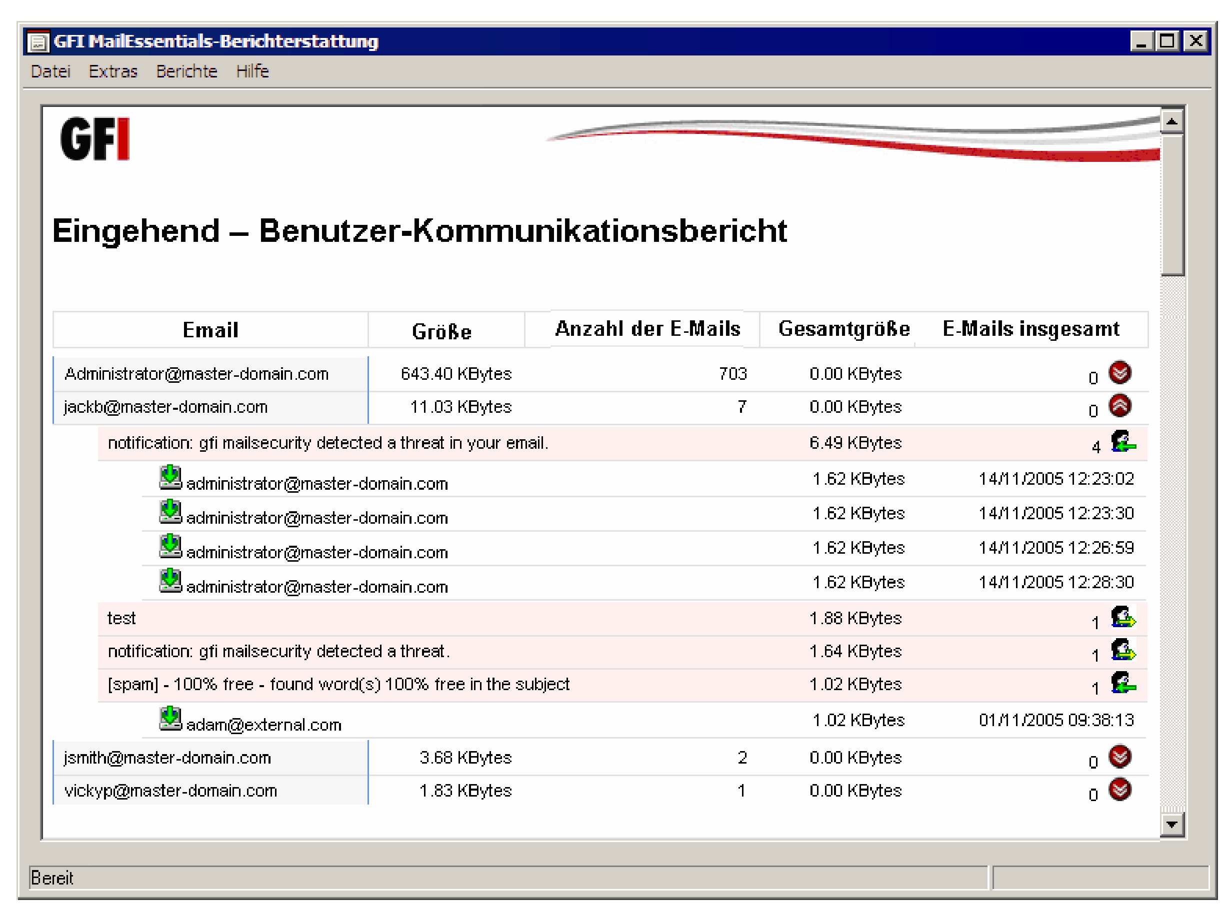


Bild 11 - Der Bericht Benutzerkommunikation zeigt eine genaue E-Mail-Analyse.

Berichtstyp

- **Berichtstyp:** Geben Sie an, ob Sie einen Bericht für die eingehenden E-Mails, die ausgehenden E-Mails oder beide erstellen wollen.

Berichtsoptionen

- **Sortierschlüssel:** Geben Sie an, ob der Bericht nach E-Mail-Adresse, nach Anzahl der E-Mails oder nach Gesamtgröße der E-Mails sortiert werden sollte.
- **Benutzer hervorheben:** Identifizieren Sie Benutzer, die ungewöhnlich viele oder ungewöhnlich große E-Mails empfangen oder versendet haben.
- **Nur wichtige anzeigen:** Zeigen Sie nur die wichtigsten Benutzer in dem Bericht an.
- **Mehrseitiger Bericht:** Geben Sie an, wie viele Benutzer pro Seite angezeigt werden sollen.

Filteroptionen

- **Spezifische E-Mail:** Beschränken Sie den Bericht auf eine bestimmte E-Mail-Adresse.
- **Datumsbereich:** Beschränkt den Bericht auf einen bestimmten Datumsbereich.

Klicken Sie bei Auswahl der betreffenden Optionen auf die Schaltfläche **Bericht** um den Bericht zu erstellen.

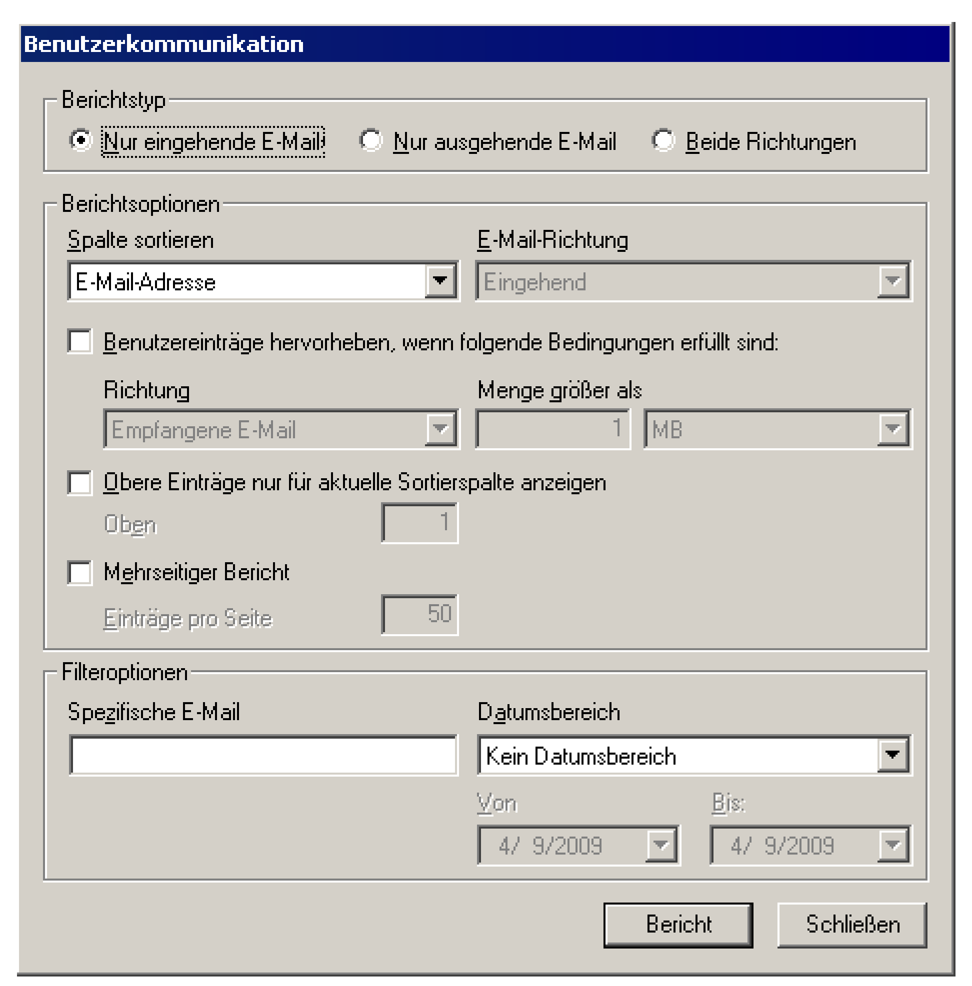


Bild 12 - Filterdialog "Benutzer-Kommunikation"

Sonstige Optionen

- Ausschluss von Benutzern aus Berichten

  Mit dem Tool zum Ausschluss von Benutzern können Benutzer aus Berichten ausgeblendet werden.

  Klicken Sie auf **Tools ► Benutzerausschlussliste** und dann auf die Schaltfläche **Hinzufügen**, damit Sie die SMTP-E-Mail-Adresse für den Benutzer, der bei Berichten ignoriert werden soll, **hinzufügen** oder **entfernen** können.

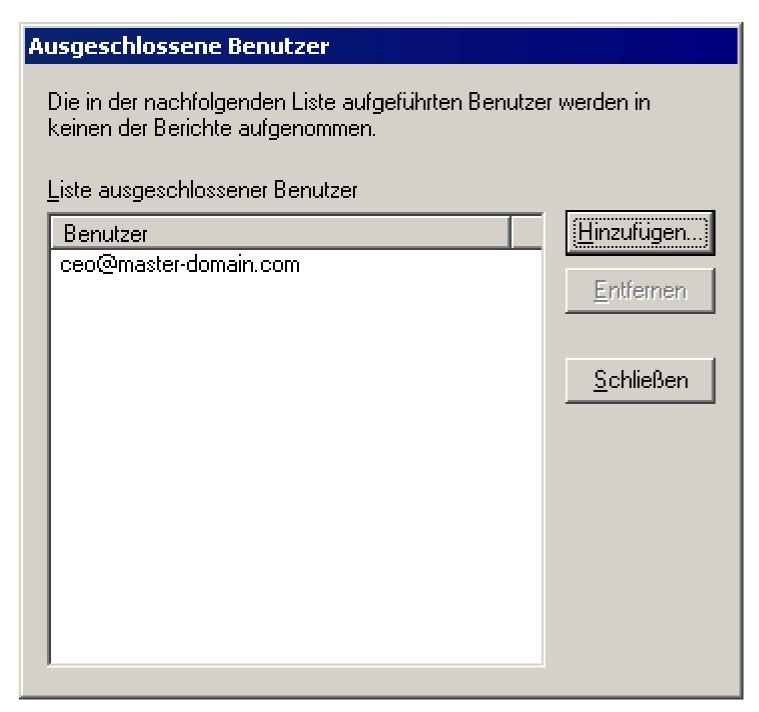


Bild 13 - Der Dialog "Ausgeschlossene Benutzer"

Such-Tool

Mit dem Such-Tool können Sie Text-Strings in Berichten finden.

Geben Sie in der Menüoption **Tools ► Suchen** die Text-Strings ein, die gefunden werden sollen, und klicken Sie dann zur Suche auf **Nächsten suchen**.

4 Routineadministration

GFI MailEssentials blockiert fast alle empfangenen Spam-E-Mails. Wie bei jeder Anti-Spam-Lösung können jedoch auch zulässige E-Mails als Spam erkannt werden (falsch-positive Ergebnisse) oder Spam-E-Mails werden nicht als Spam erkannt (falsch-negative Ergebnisse). Davon ausgehend, dass Spam einen hohen Prozentsatz am gesamten E-Mail-Fluss eines Unternehmens ausmacht (meistens zwischen 70 und 90 %), handelt es sich täglich um tausende zu verwaltende E-Mails. Ein System, das allein durch den Administrator verwaltet wird, ist daher unpraktisch. GFI MailEssentials kann so konfiguriert werden, dass Endbenutzer selbst bestimmen können, ob E-Mails fälschlicherweise als Spam oder zulässig klassifiziert wurden.

4.1 Verwenden der Quarantäne

Die Quarantäne von GFI MailEssentials ist ein zentraler Speicher, wo alle als Spam erkannten, eingehenden E-Mails für einige Tage verbleiben. Dies stellt sicher, dass Benutzer keinen Spam empfangen, und die für die Verarbeitung dieser E-Mails verwendeten Ressourcen auf dem Mailserver werden reduziert.

Dieses Kapitel enthält Informationen zur Verwendung und Wartung des Quarantänespeichers. Weitere Informationen zur Konfiguration der Quarantäne finden Sie im Abschnitt **Konfigurieren der Quarantäne** in diesem Handbuch.

Administratoren und E-Mail-Benutzer können die E-Mails in Quarantäne anzeigen, indem Sie mit einem Webbrowser auf die Quarantäneoberfläche zugreifen. GFI MailEssentials kann außerdem reguläre E-Mail-Berichte an E-Mail-Benutzer senden, um über die blockierten E-Mails zu informieren.

HINWEIS: Nur Administratoren haben Zugriff auf alle Spam-E-Mails in Quarantäne. Normale E-Mail-Benutzer können nur auf blockierte E-Mails zugreifen, die an sie selbst adressiert waren. Informationen zum Konfigurieren von Berechtigungen finden Sie im Kapitel **Konfigurieren der Quarantäne** dieses Handbuchs.

4.1.1 Quarantäneverwaltung

Die Seite der Quarantäneverwaltung zeigt statistische Informationen und bietet eine Quarantänesuchfunktion. So greifen Sie auf die Quarantäneverwaltung zu:

- GFI MailEssentials - Konfiguration - Öffnen Sie Anti-Spam ► Quarantäne.
- **Web-Oberfläche** - Benutzer können über einen Webbrowser auf die Seite der Quarantäneverwaltung zugreifen. Geben Sie die konfigurierte Adresse in folgendem Format ein:

  http://<*GFI MailEssentials-Servername* >/<*Virtuelles Verzeichnis der Quarantäne*>

  Beispiel 1: http://GFIserver/SpamQuarantine

  Beispiel 2: Wenn das virtuelle Verzeichnis der Quarantäne für den Webzugriff konfiguriert wurde: http://www.mydomain.com/SpamQuarantine

  HINWEIS: Falls das virtuelle Verzeichnis der durch SSL gesichert ist, verwenden Sie https:// anstelle von http://.

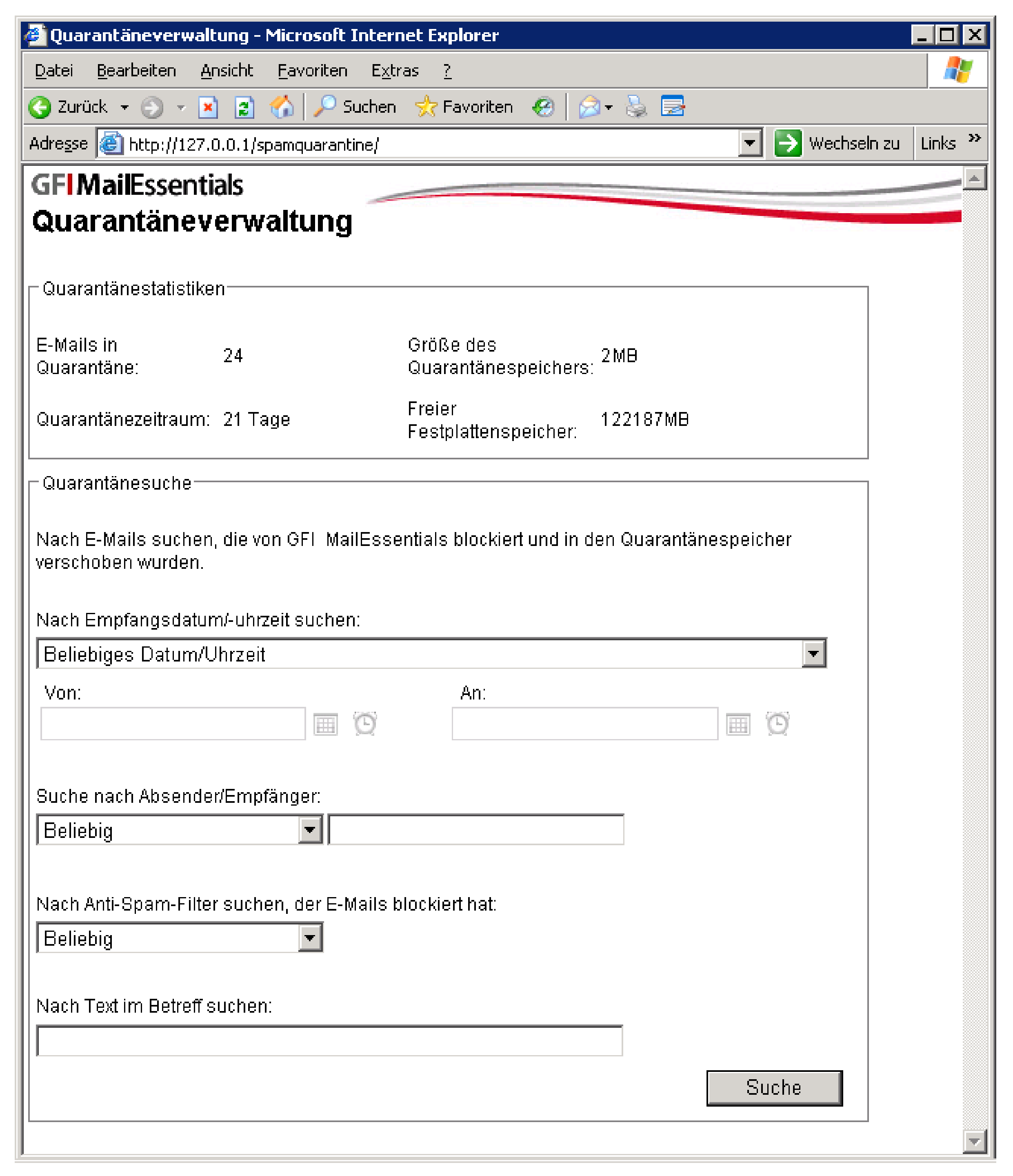


Bild 14 - Seite der Quarantäneverwaltung

Im Bereich für Quarantänestatistiken wird Folgendes angezeigt:

» **E-Mails in Quarantäne** - Anzahl der E-Mails im Quarantänespeicher.

» **Quarantänezeitraum** - Anzahl der Tage, die die E-Mails im Quarantänespeicher verbleiben.

» **Größe des Quarantänespeichers** - Speicherplatz auf der Festplatte, der vom Quarantänespeicher eingenommen wird, um Spam-E-Mails und Metadaten zu speichern.

» **Freier Festplattenspeicher** - Freier Speicherplatz auf der Partition, wo der Quarantänespeicher abgespeichert ist. Falls dieser Wert unter 512 MB liegt, wird die Quarantänefunktion gestoppt. Spam-E-Mails werden gekennzeichnet und dem Empfängerpostfach zugestellt, bis der freie Speicherplatz größer als 512 MB ist.

HINWEIS: Weitere Informationen zum Ändern des Speicherorts des Quarantänespeichers oder der Anzahl der Speichertage finden Sie im Abschnitt Konfigurieren der Quarantäne in diesem Handbuch.

Durchsuchen von E-Mails in Quarantäne

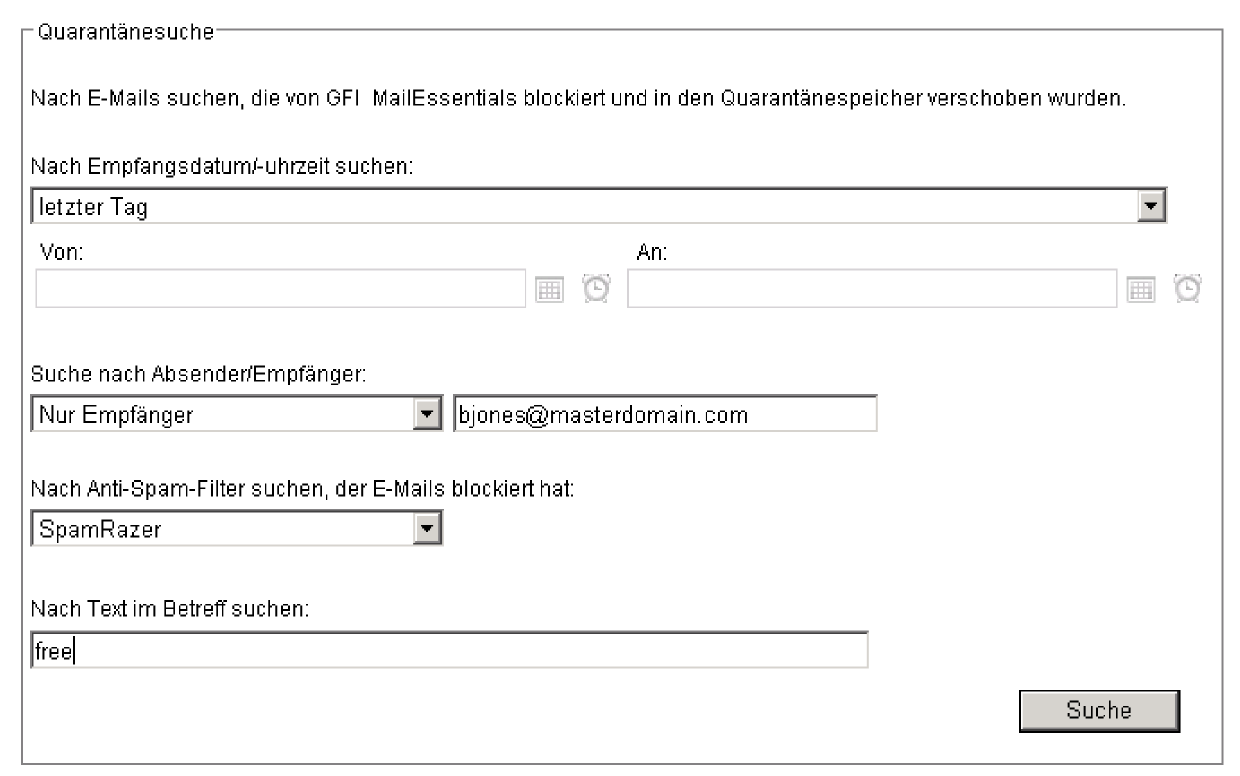


Bild 15 - Quarantänensuche

HINWEIS: Nur Administratoren können alle Spam-E-Mails in Quarantäne durchsuchen. Normale E-Mail-Benutzer können nur blockierte E-Mails durchsuchen, die an sie selbst adressiert waren.

Im Bereich der Quarantänensuche auf der Seite der Quarantänenverwaltung können folgende Suchkriterien festgelegt werden:

- Datum / Uhrzeit, wann die E-Mail empfangen wurde,
- Absender und/oder Empfänger,
- Anti-Spam-Filter, der die E-Mail blockiert hat,
- Text im Betreff.

Klicken Sie auf **Suche**, um die Suchergebnisse anzuzeigen.

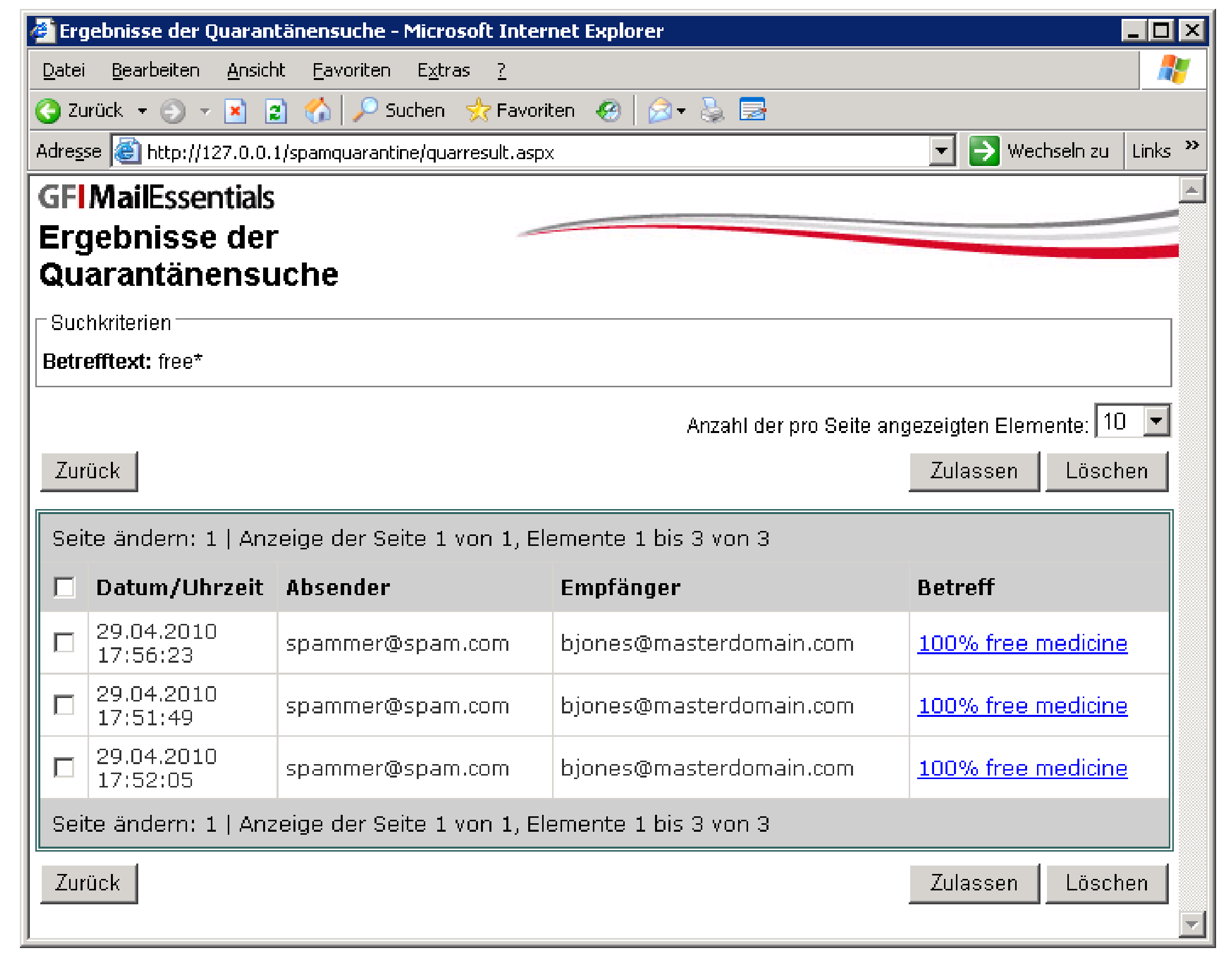


Bild 16 - Ergebnisse der Quarantänensuche

Wählen Sie E-Mails aus, bei denen es sich nicht um Spam handelt, und klicken Sie auf **Zulassen**.

Administratoren können auch Absender von E-Mails zu einer Whitelist hinzufügen, die fälschlicherweise als Spam gekennzeichnet wurden. Klicken Sie auf den Betreff der E-Mail, um eine Vorschau der E-Mail anzuzeigen, und dann auf **Zur Whitelist hinzufügen und zulassen**.

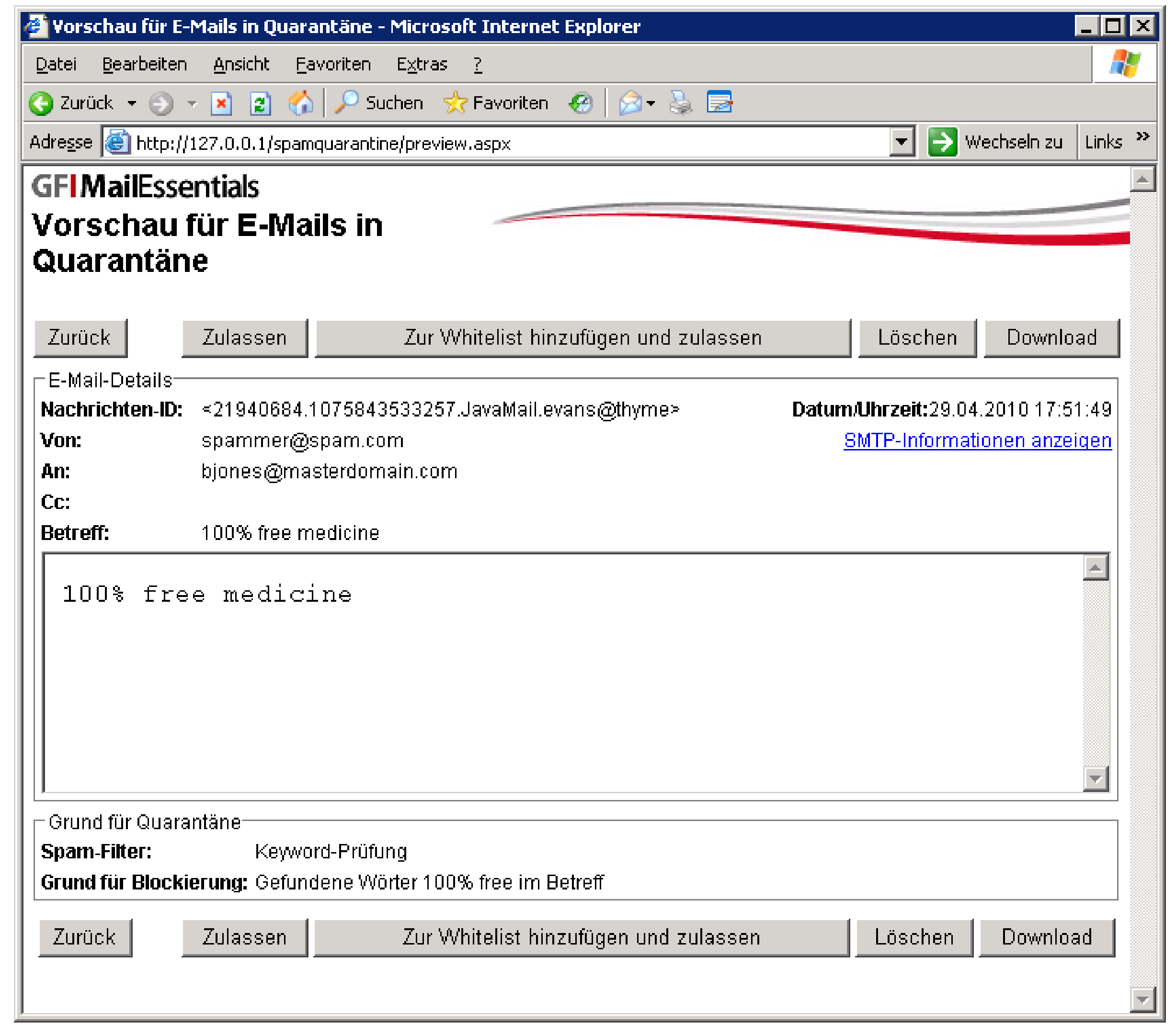


Bild 17 - Anzeigen einer E-Mail in Quarantäne

4.1.2 Benutzerquarantäneberichte

Sie können GFI MailEssentials so konfigurieren, dass regelmäßig Quarantäneberichte an E-Mail-Benutzer gesendet werden. Diese E-Mail enthält eine Liste der durch GFI MailEssentials blockierten E-Mails seit dem letzten Quarantänebericht.

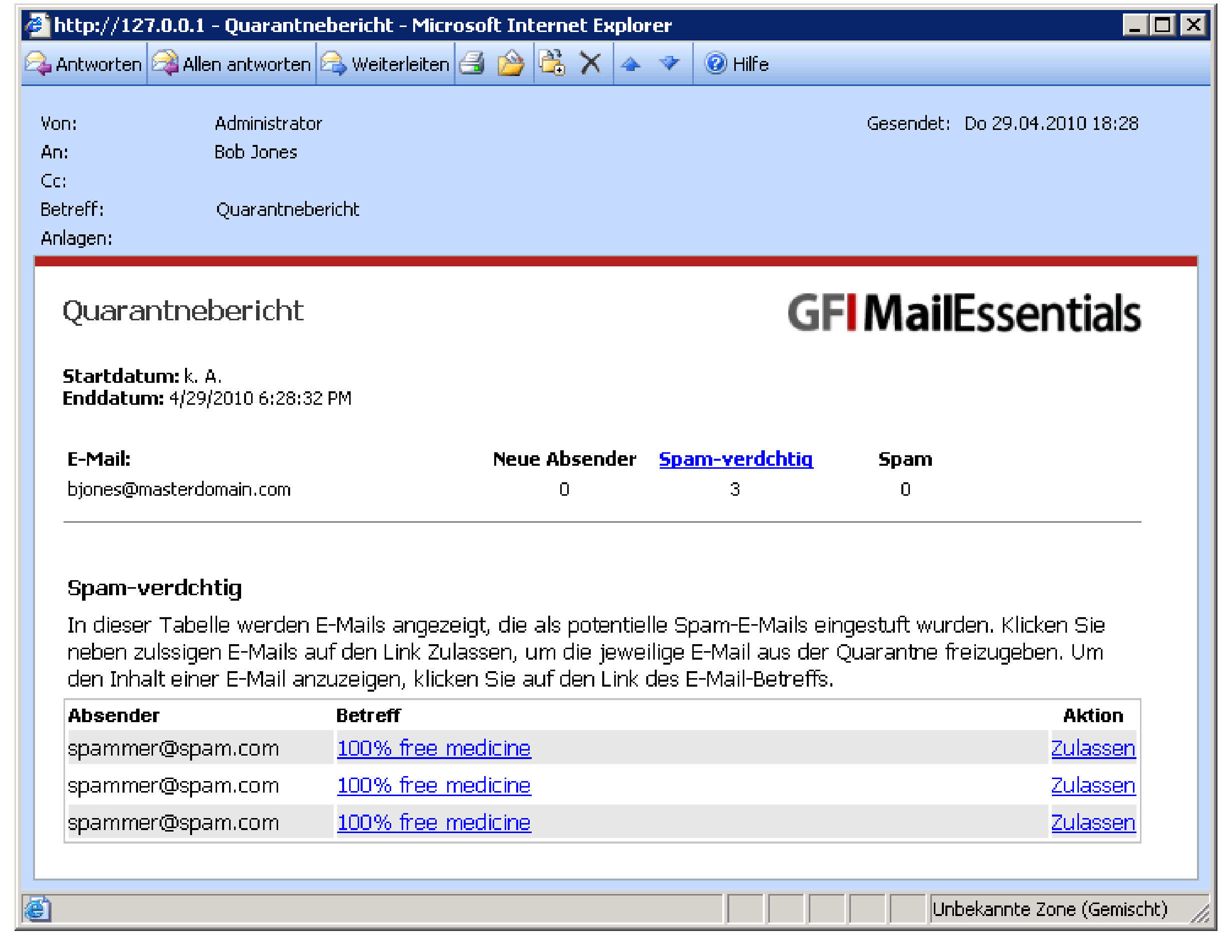


Bild 18 - Quarantäne-E-Mail-Bericht

Der Empfänger kann die blockierten E-Mails anzeigen, und E-Mails zulassen, die fälschlicherweise als Spam gekennzeichnet wurden. Wählen Sie dazu die E-Mails aus, bei denen es sich nicht um Spam handelt, und klicken Sie auf **Zulassen**.

Sie können auch auf den E-Mail-Betreff klicken, um eine Vorschau der E-Mail im Webbrowser anzuzeigen.

HINWEIS: Falls der E-Mail-Client so konfiguriert ist, dass E-Mails nur im Klartextformat angezeigt werden, können E-Mails nicht direkt aus dem Quarantäne-E-Mail-Bericht angezeigt werden. Der Bericht weist den Benutzer darauf hin, dass E-Mails von GFI MailEssentials blockiert wurden, und stellt einen Link bereit, über den die Quarantäneoberfläche in einem Webbrowser gestartet werden kann. Der Benutzer kann dann Spam-E-Mails im Webbrowser anzeigen und gegebenenfalls zulassen.

4.2 Überprüfen öffentlicher Ordner

4.2.1 Überprüfen von Spam klassifizierten Mitteilungen

1. Wenn Spam-E-Mails an das Postfach zugestellt werden (Posteingang, Junk-Mail-Ordner oder einem benutzerdefinierten Ordner), müssen die einzelnen E-Mail-Benutzer darauf hingewiesen werden, regelmäßig die Spam-E-Mails durchzuschauen.

2. Wenn zulässige E-Mails fälschlicherweise als Spam gekennzeichnet wurden (falsch-positive Ergebnisse), beziehen Sie sich auf den unteren Abschnitt Umgang mit zulässigen E-Mails.

3. Wenn Spam-E-Mails nicht gekennzeichnet wurden (falsch-negative Ergebnisse), beziehen Sie sich auf den unteren Abschnitt Umgang mit Spam-Mails.

4.2.2 Umgang mit zulässigen E-Mails

Wie jede Anti-Spam-Lösung braucht auch GFI MailEssentials eine gewisse Zeit, bis die optimale Spam-Filterbedingungen eingestellt sind. Solange dies noch nicht der Fall ist, ist es möglich, dass zulässige E-Mails als Spam identifiziert werden.

In solchen Fällen sollten die Benutzer E-Mails, die fälschlicherweise als Spam identifiziert wurden, in den Ordner **Zur Whitelist hinzufügen** bzw. in den Ordner **Dies ist eine zulässige E-Mail** schieben, damit GFI MailEssentials 'lernt', dass die betreffende E-Mail keine Spam-Mail ist.

Wichtige Hinweise

In Microsoft Outlook verschieben Sie E-Mails per Drag&Drop in den gewünschten Ordner. Um eine Kopie der E-Mail zu behalten, halten Sie die Taste **STRG** gedrückt um die E-Mail zu kopieren und nicht nur zu verschieben.

Hinzufügen von Absendern oder Newslettern zur Whitelist.

1. Suchen Sie unter den öffentlichen Ordnern den Ordner **GFI Anti-Spam-Ordner ► Zur Whitelist hinzufügen**.

2. Schieben Sie per Drag&Drop E-Mails oder Newsletter in den öffentlichen Ordner **Zur Whitelist hinzufügen**.

Hinzufügen von Diskussionslisten zur Whitelist

Diskussionslisten werden oft ohne die Empfänger-E-Mail-Adresse in dem Feld MIME TO versendet und daher als Spam gekennzeichnet. Um solche Diskussionslisten zu empfangen, schieben Sie die E-Mail-Adressen dieser gültigen Listenabsender in die Whitelist.

1. Suchen Sie unter den öffentlichen Ordnern den Ordner **GFI AntiSpam-Ordner ► Ich möchte diese Diskussionsliste**.

2. Schieben Sie Diskussionslisten per Drag&Drop in den öffentlichen Ordner **Ich möchte diese Diskussionsliste**.

HAM zur Datenbank zulässiger E-Mails hinzufügen.

1. Suchen Sie unter den öffentlichen **GFI AntiSpam-Ordner ► Diese E-Mail ist kein Spam**.

2. Schieben Sie die E-Mails per Drag&Drop in den öffentlichen Ordner **Diese E-Mail ist kein Spam**.

4.2.3 Umgang mit Spam-Mails

Wenn GFI MailEssentials beginnt, Spam-Mails mit der Standardinstallation zu identifizieren, kann es Fälle geben, in denen Spam-Mails unerkannt in das Benutzerpostfach gelangen. In der Regel kommt dies vor, weil Konfigurationseinstellungen noch nicht definiert wurden oder weil es sich um eine neue Form von Spam-Mails handelt, die GFI MailEssentials noch nicht kennt. In beiden Fällen beseitigen Sie solche Situationen, wenn Sie GFI MailEssentials so konfigurieren, dass diese Spam-Mails zurückgehalten werden.

HINWEIS: Wie Sie Probleme im Zusammenhang mit E-Mails lösen, die nicht als Spam erkannt wurden, finden Sie in dem Kapitel Problembehandlung & Support in diesem Handbuch.

Die Benutzer sollten in solchen Fällen diese E-Mails in die Ordner **Zur Blockliste hinzufügen** und **Diese E-Mail ist Spam** verschieben, damit GFI MailEssentials 'lernt', dass die betreffende E-Mail eine Spam-Mail ist.

Wichtige Hinweise

1. In Microsoft Outlook verschieben Sie E-Mails per Drag&Drop in den gewünschten Ordner. Um eine Kopie der E-Mail zu behalten, halten Sie die Taste **STRG** gedrückt um die E-Mail zu kopieren und nicht nur zu verschieben.

2. Weitere Informationen, wie Sie automatisch die GFI Anti-Spam Ordner erstellen, finden Sie unter Scannen öffentlicher Ordner in diesem Handbuch.

Hinzufügen von Absendern zur Blockliste

1. Suchen Sie unter den öffentlichen Ordnern den Ordner **GFI AntiSpam-Ordner ► Zur Blocklist hinzu**.

2. Verschieben Sie per Drag&Drop E-Mails in den öffentlichen Ordner **Zur Blocklist hinzu**.

Hinzufügen von Spam-Mails zur Spam-Datenbank

1. Suchen Sie unter den öffentlichen Ordnern den **GFI AntiSpam-Ordner ► Diese E-Mail ist Spam**.

2. Verschieben Sie die Spam-Mail per Drag&Drop in den öffentlichen Ordner **Diese E-Mail ist Spam**.

5 Konfigurieren der Anti-Spam-Optionen

5.1 Spam-Filter

GFI MailEssentials nutzt verschiedene Spam-Filter zur Identifizierung von Spam:

FILTER	BESCHREIBUNG	STANDARD-MÄßIG AKTIVIERT
SpamRazer	Ein Spam-Filter, der erkennt, ob eine E-Mail Spam ist. Dazu wird die E-Mail-Herkunft, der Inhalt der Nachricht und deren Transportweg analysiert.	Ja
Directory Harvesting	Das Modul stoppt E-Mails, die nach dem Zufallsprinzip erzeugt an einen Server gesendet werden, für die aber meist keine Benutzer existieren.	Nein
Phishing	Dieser Filter blockiert E-Mails, die Links in den Nachrichtentexten enthalten, die auf bekannte Phishing-Sites zeigen oder typische Phishing-Keywords enthalten.	Ja
Sender Policy Framework	Dieser Filter stoppt E-Mails, die von Domänen stammen, die in den SPF-Records nicht autorisiert wurden.	Nein
Auto-Whitelist	Wenn an diese Adressen eine E-Mail gesendet wird, werden Spam-Filter automatisch ignoriert.	Ja
Whitelists	Eine benutzerdefinierte Liste sicherer E-Mail-Adressen	Ja
E-Mail-Blocklist	Eine benutzerdefinierte Liste gesperrter E-Mail-Nutzer oder Domänen.	Ja
IP-DNS-Blocklist	Prüft, ob die empfangene E-Mail von Absendern stammt, die in einer öffentlichen DNS-Blockliste bekannter Spammer enthalten sind.	Ja
URI-DNS-Blocklist	Dieser Filter stoppt E-Mails, die Links zu Domänen enthalten, die in den öffentlichen Spam-URL-Blocklists enthalten sind, beispielsweise sc.surbl.org.	Ja
Header-Prufüng	Dieses Modul analysiert die einzelnen Felder im Header durch Vergleich mit dem SMTP- und MIME-Feld.	Ja
Keyword-Prufüng	Spam-Mails werden anhand gesperrter Keywords in der E-Mail-Überschrift oder in der E-Mail-Nachricht identifiziert.	Nein
Neue Absender	E-Mails, die von Absendern stammen, an die noch nie eine E-Mail gesendet wurde.	Nein
Bayes'sche Analyse	Ein Spamverfahren, bei dem nach Training durch die Benutzer Spam-Mails mit statistischen Verfahren identifiziert werden.	Nein
Greylist	Erkennt E-Mails von nicht RFC-konformen Mailservern, die normalerweise von Spammern verwendet werden.	Nein

SpamRazer

SpamRazer ist der wichtigste Spam-Filter von GFI und standardmäßig nach der Installation aktiviert. Für SpamRazer werden häufige Aktualisierungen angeboten um schnell auf neue Spam-Trends zu reagieren.

HINWEIS: SpamRazer ist außerdem auch der Spam-Filter, der NDR-Spam blockiert. Weitere Informationen über GFI MailEssentials und NDR-Spam finden Sie unter:

http://kbase.gfi.com/showarticle.asp?id=KBID003322

Konfiguration von SpamRazer

HINWEIS 1: Eine Deaktivierung von SpamRazer wird NICHT empfohlen.

HINWEIS 2: GFI MailEssentials lädt SpamRazer-Aktualisierungen von folgender Adresse herunter: http://sn92.mailshell.net

1. Wählen Sie **Anti-Spam** ► **Anti-Spam-Filter** ► **SpamRazer** ► **Eigenschaften**.

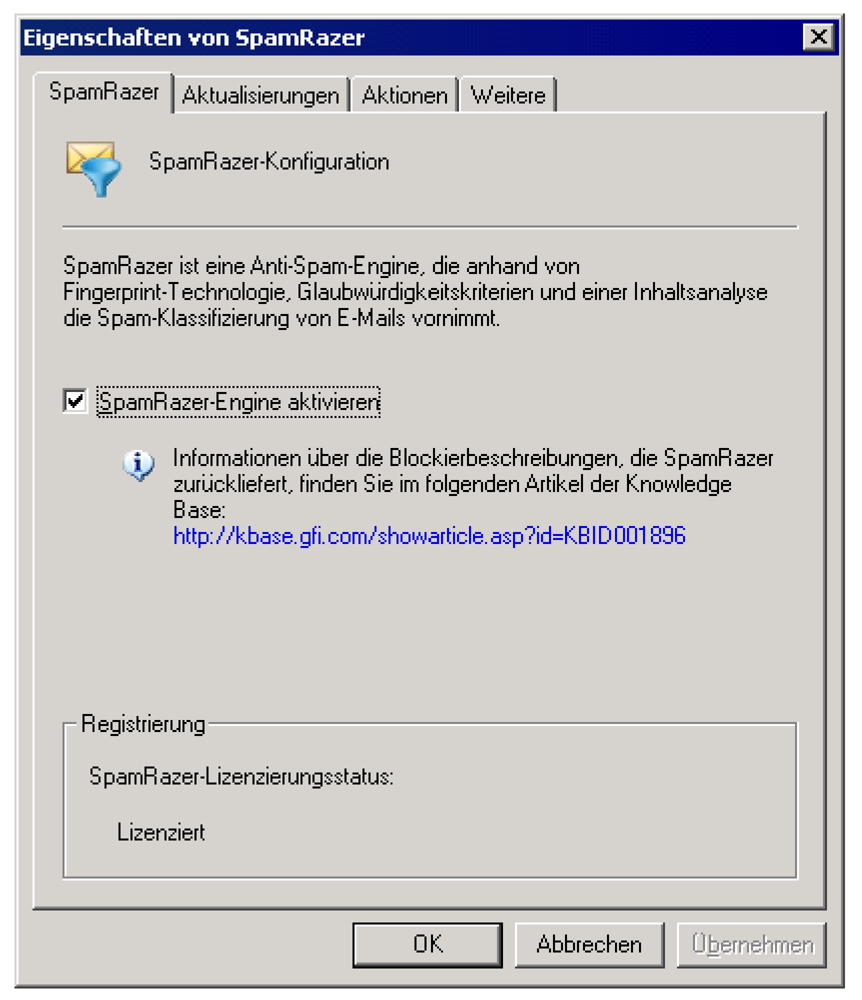


Bild 19 - SpamRazer-Eigenschaften

2. Führen Sie auf der Registerkarte **SpamRazer** eine der folgenden Aktionen aus:

» Aktivieren/deaktivieren Sie das Kontrollkästchen **SpamRazer aktivieren** um SpamRazer zu aktivieren oder zu deaktivieren.

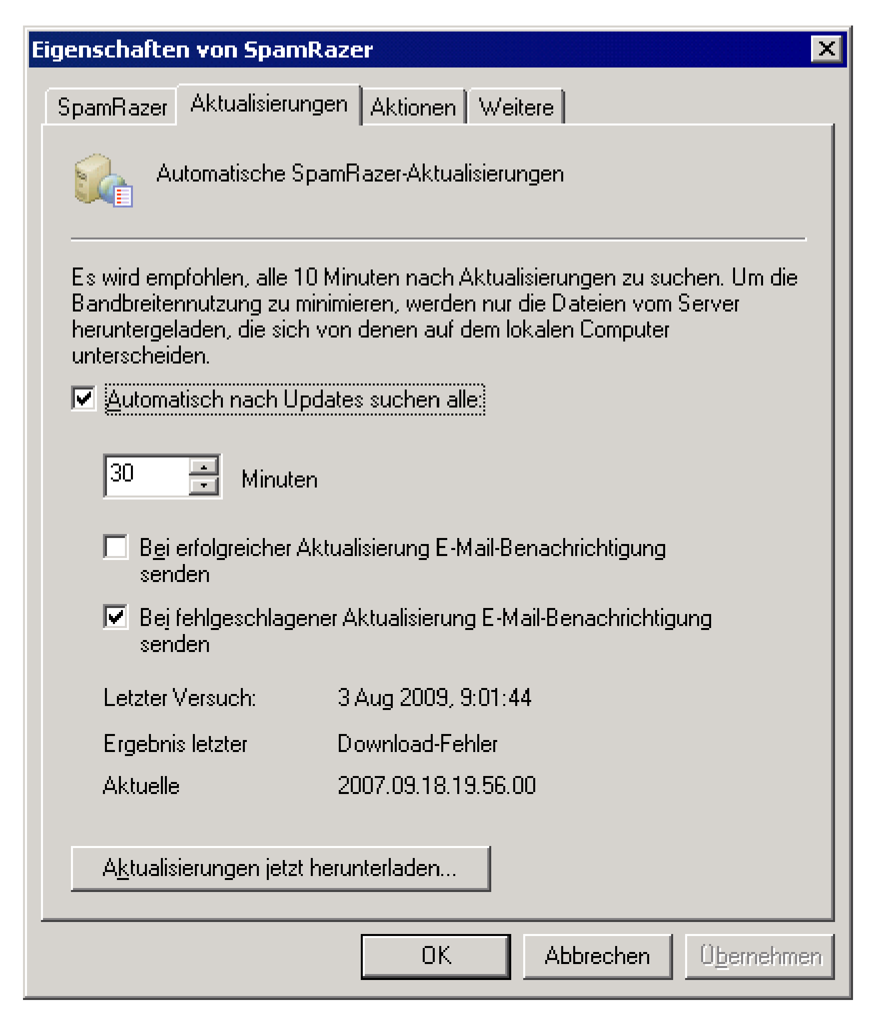


Bild 20 - Automatische SpamRazer-Aktualisierungen

3. Führen Sie auf der Registerkarte **Aktualisierungen** eine der folgenden Aktionen aus:

- Aktivieren oder deaktivieren Sie das Kontrollkästchen **Automatisch nach Updates suchen** um GFI MailEssentials so zu konfigurieren, dass das Programm automatisch SpamRazer-Updates sucht und diese herunterlädt. Geben Sie das Zeitintervall für die Prüfung auf Updates in Minuten an.

  HINWEIS: Wir empfehlen, diese Option für SpamRazer aktiviert zu lassen, damit die aktuellsten Spam-Trends effektiver erkannt werden.

- Aktivieren/deaktivieren Sie das Kontrollkästchen **Benachrichtigungs-E-Mail versenden, wenn ein Update erfolgreich war**, damit Sie per E-Mail informiert werden, ob neue Updates heruntergeladen sind.
- Aktivieren/deaktivieren Sie das Kontrollkästchen **Benachrichtigungs-E-Mail versenden wenn das Update fehlschlägt**, damit Sie informiert werden, wenn ein Download oder eine Installation fehlgeschlagen ist.
- Klicken Sie auf **Updates jetzt herunterladen ...** um die Updates herunterzuladen.

HINWEIS: Hinweise zum Herunterladen von Updates über einen Proxyserver finden Sie unter Automatischer Updates in diesem Handbuch.

4. Klicken Sie auf die Registerkarte **Aktionen** oder **Weitere** um die Aktionen auszuwählen, die bei Spam-Nachrichten durchgeführt werden sollen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails in diesem Handbuch.

5. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

Phishing

Phishing ist ein E-Mail-Verfahren, das die E-Mail-Benutzer bewegen soll, Spammern persönliche Daten preiszugeben. Eine Phishing-E-Mail ist meist so gestaltet, dass sie einer offiziellen E-Mail

von einer vertrauenswürdigen Stelle, beispielsweise einer Bank, ähnelt. Phishing-E-Mails enthalten in der Regel Anweisungen, dass Benutzer sensitive Informationen, beispielsweise Online-Banking-Zugangsdaten oder Kreditkartendaten, bestätigen sollen. Phishing-E-Mails enthalten in der Regel einen Phishing Uniform Ressource Identifier (URI), den der Leser aufrufen soll um bestimmte sensitive Informationen auf einer Phishing-Site einzugeben. Diese Seite, auf die die Phishing-URI zeigt, kann eine Kopie einer offiziellen Website sein, wird jedoch von demjenigen kontrolliert, der die Phishing-E-Mails versendet hat. Wenn der Benutzer sensitive Daten auf der Phishing-Website eingibt, werden die Daten gesammelt und beispielsweise genutzt um Geld von Bankkonten abzuheben.

Die Funktion Phishing erkennt Phishing-E-Mails, da sie die in der E-Mail erhaltene URI mit einer Datenbank bekannter URIs vergleicht, die für Phishing-Angriffe verwendet wurden. Die Funktion Phishing sucht außerdem in den URIs nach typischen Phishing-Keywords.

Der Phishing-Filter ist standardmäßig nach der Installation aktiviert.

Konfiguration des Phishing

HINWEIS 1: Eine Deaktivierung des Phishing wird NICHT empfohlen.

1. Wählen Sie **Anti-Spam** ► **Anti-Spam-Filter** ► **Phishing** ► **Eigenschaften**.

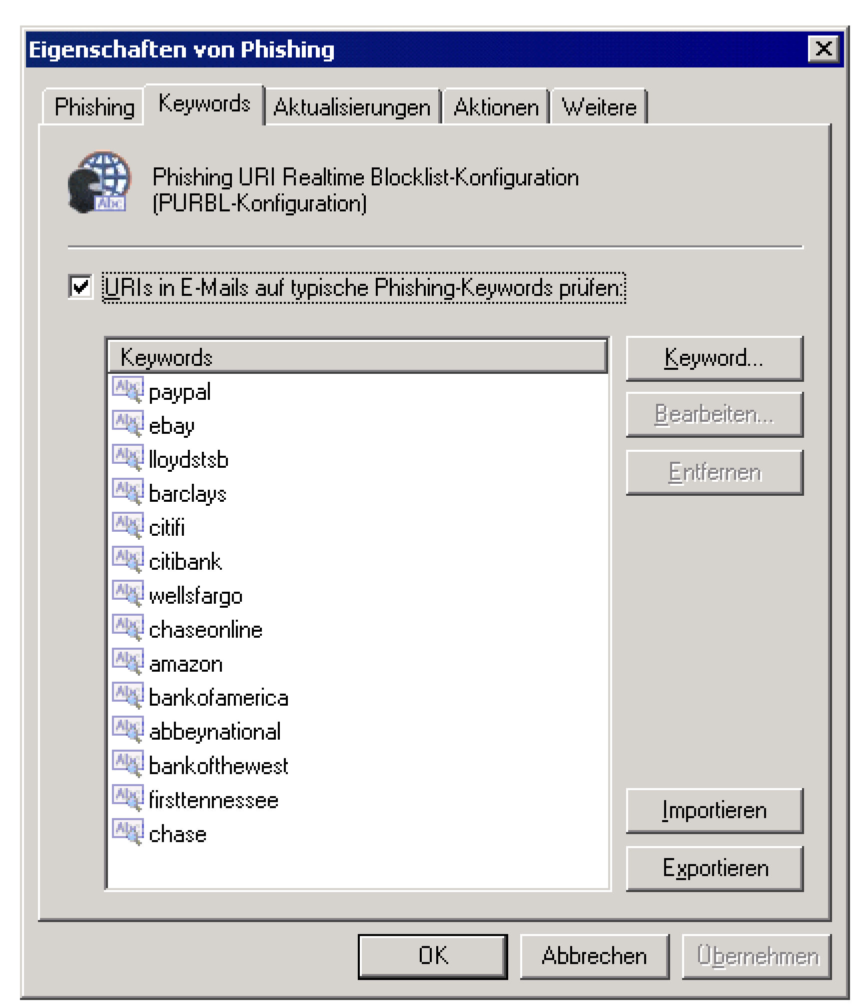


Bild 21 - Phishing-Keywords

2. Klicken Sie auf der Registerkarte **Phishing** auf folgende Aktionen:

   - Aktivieren/deaktivieren Sie die Option **E-Mails auf URIs bekannter Phishing-Websites prüfen** um PURBL zu aktivieren oder zu deaktivieren.

3. Führen Sie auf der Registerkarte **Keywords** folgende Aktionen aus:

   - Aktivieren oder deaktivieren Sie die Option **URIs in E-Mails auf typische Phishing-Keywords prüfen** um typische Phishing-Keywords zu aktivieren oder zu deaktivieren.

- Klicken Sie auf die Schaltfläche **Keyword** und geben Sie die Keywords in dem Dialog **Keyword eingeben** ein um Keywords in dem PURBL-Filter zu ergänzen.
- Wählen Sie ein Keyword aus und klicken Sie auf **Bearbeiten** oder **Entfernen** um das eingegebene Keyword zu bearbeiten oder aus dem Phishing-Filter zu entfernen.
- Klicken Sie auf **Exportieren** um die aktuelle Keyword-Liste im XML-Format zu exportieren.
- Klicken Sie auf **Importieren** um die zuvor in XML exportierte Keyword-Liste wieder zu importieren.

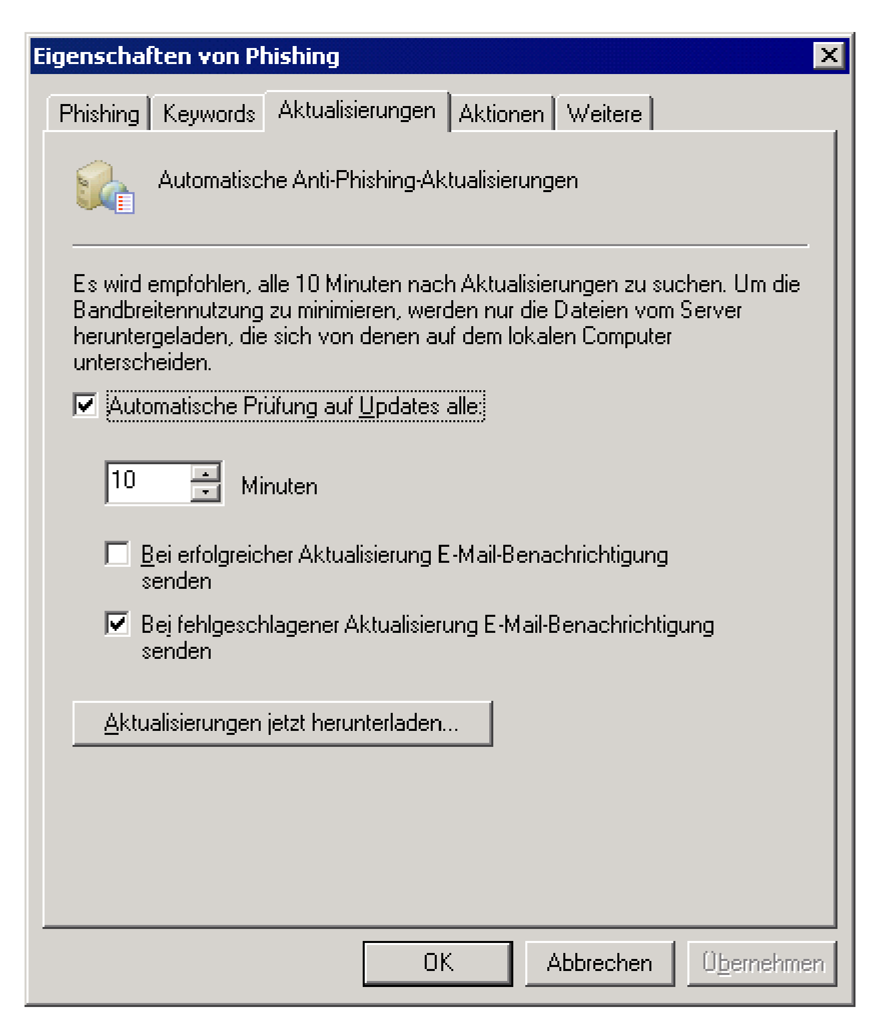


Bild 22 - Automatische Anti-Phishing-Aktualisierungen

4. Führen Sie auf der Registerkarte **Aktualisierungen** eine der folgenden Aktionen aus:

- Aktivieren/deaktivieren Sie das Kontrollkästchen **Automatisch auf Aktualisierungen prüfen** um die automatische Prüfung und das Herunterladen von Anti-Phishing-Aktualisierungen zu aktivieren bzw. zu deaktivieren.

  HINWEIS: Wir empfehlen, unbedingt diese Option zu aktivieren, da durch häufige Aktualisierungen Phishing die jüngsten Phishing-E-Mails effektiver erkannt werden.
- Aktivieren/deaktivieren Sie das Kontrollkästchen **Benachrichtigungs-E-Mail versenden, wenn eine Aktualisierung erfolgreich war**, damit Sie per E-Mail informiert werden, ob neue Aktualisierungen heruntergeladen sind.
- Aktivieren/deaktivieren Sie das Kontrollkästchen **Benachrichtigungs-E-Mail versenden wenn die Aktualisierung fehlschlägt**, damit Sie informiert werden, wenn ein Download oder eine Installation fehlgeschlagen ist.

HINWEIS: Hinweise zum Herunterladen von Updates über einen Proxyserver finden Sie unter Automatischer Updates in diesem Handbuch

5. Klicken Sie auf die Registerkarte **Aktionen** oder **Weitere** um die Aktionen für als Phishing-E-Mails identifizierte Nachrichten auszuwählen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt **Spam-Aktionen - Umgang mit Spam-Mails** in diesem Handbuch.

6. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

Directory Harvesting

Directory Harvesting-Angriffe nutzen bekannte E-Mail-Adressen als Vorlage um weitere E-Mail-Adressen zu erzeugen, die dann an Firmen- oder ISP-E-Mail-Server gesendet werden. Die Spammer senden nach dem Zufallsprinzip erzeugte E-Mail-Adressen; zwar können einige E-Mail-Adressen mit echten E-Mail-Adressen übereinstimmen, die Mehrzahl dieser Adressen ist jedoch ungültig und überlastet den E-Mail-Server des Opfers.

GFI MailEssentials stoppt diese Angriffe, indem E-Mails an Benutzer, die nicht in Active Directory oder im E-Mail-Server des Unternehmens eingetragen sind, blockiert werden.

Directory Harvesting kann entweder so konfiguriert werden, dass die Funktion ausgeführt wird, sobald die vollständige E-Mail empfangen wird oder auf SMTP-Ebene, das heißt, beim Empfang der IP des Absenders der E-Mail und der Empfänger. Bei einer SMTP-Filterung wird die E-Mail-Verbindung beendet und damit ein komplettes Herunterladen der E-Mail verhindert um Bandbreite und Verarbeitungskapazität zu sparen. In diesem Fall wird die Verbindung sofort unterbrochen und die E-Mails müssen nicht weitere Spam-Filter passieren.

Dieser Filter ist standardmäßig nach Installation von GFI MailEssentials NICHT aktiviert.

Konfiguration von Directory Harvesting

Directory harvesting konfigurieren Sie in zwei Phasen:

Phase 1 - Konfiguration der Eigenschaften von Directory Harvesting

Phase 2 - Auswahl des Verfahrens für Directory Harvesting

Phase 1 - Konfiguration der Eigenschaften von Directory Harvesting

1. Klicken Sie auf **Anti-Spam ► Anti-Spam-Filter ► Directory Harvesting ►** Eigenschaften und dann auf die Option **Schutz vor Directory Harvesting** aktivieren.

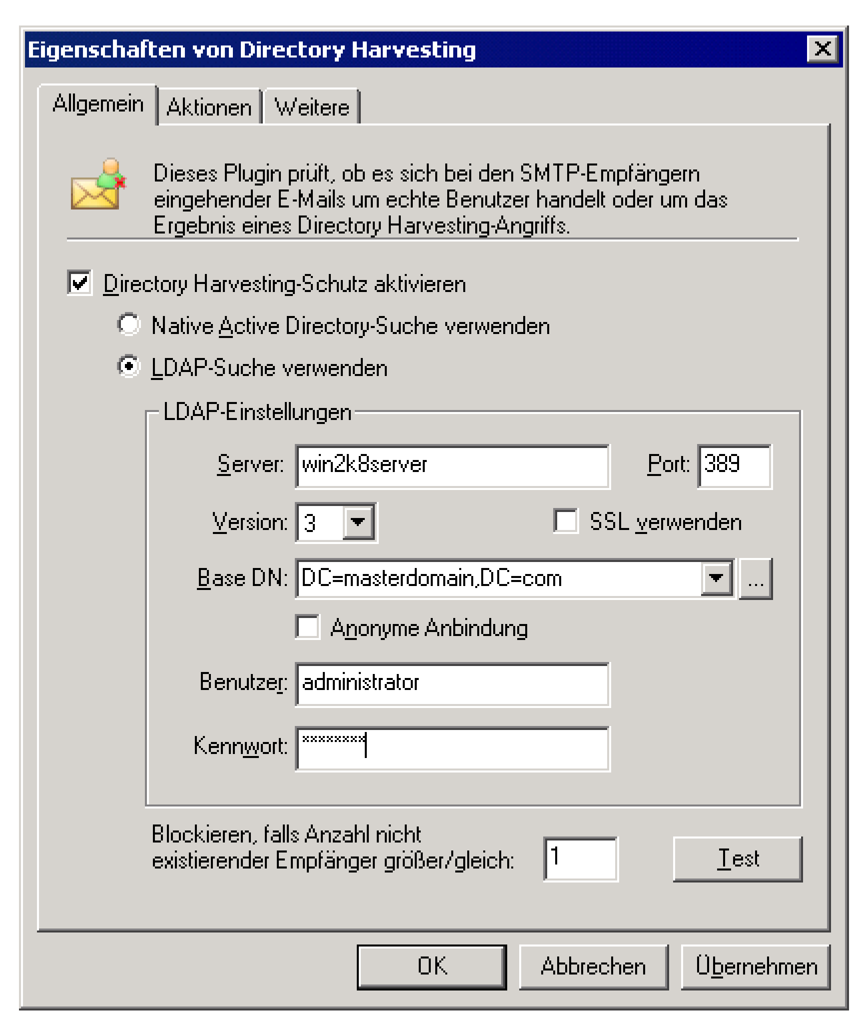


Bild 23 - Die Funktion Directory Harvesting

2. Wählen Sie das gewünschte Suchverfahren aus:

- **Verwenden Sie die Option Native Active Directory-Suche**, wenn GFI MailEssentials im Active Directory-Benutzermodus installiert ist.

  HINWEIS 1: Ist GFI MailEssentials im Active Directory-Benutzermodus in einer DMZ installiert, enthält die Active Directory der DMZ in der Regel nicht alle Netzwerkbenutzer (E-Mail-Empfänger). Nutzen Sie in diesem Fall für Directory Harvesting die LDAP-Suche.

  HINWEIS 2: Befindet sich GFI MailEssentials vor einer Firewall, kann mit der Funktion Directory Harvesting aufgrund der Firewall-Einstellungen möglicherweise keine direkte Verbindung mit dem internen Active Directory aufgebaut werden. Stellen Sie die Verbindung mit dem internen Active Directory Ihres Netzwerks über LDAP her und kontrollieren Sie, ob in Ihrer Firewall der Standard-Port 389 offen ist.

- **Konfigurieren Sie mit "LDAP Suche verwenden"** die LDAP-Einstellungen, wenn GFI MailEssentials im SMTP-Modus installiert ist. Benötigt Ihr LDAP-Server eine Authentifizierung, deaktivieren Sie die Option **Anonyme Bindung** und geben Sie die Authentifizierungsdaten für diese Funktion ein.

  HINWEIS 1: Definieren Sie die Authentifizierungsdaten im Format Domäne\Benutzer, beispielsweise Master-Domäne\Administrator.

  HINWEIS 2: In Active Directory ist der LDAP-Server in der Regel der Domänen-Controller.

3. Geben Sie für die Option **Blockieren, falls Anzahl nicht existierender Empfänger größer/gleich** die Anzahl der nicht existierenden Empfänger ein, wegen denen die E-Mail als Spam gekennzeichnet werden soll. E-Mails werden durch Directory Harvesting blockiert, falls alle Empfänger einer E-Mail ungültig sind, oder wenn die Anzahl der ungültigen Empfänger die festgelegte Anzahl übersteigt.

HINWEIS: Vermeiden Sie falsch-positive Ergebnisse, indem Sie eine angemessene Anzahl für die

Option **Blockieren, falls Anzahl nicht existierender Empfänger größer/gleich** eingeben. Dieser Wert sollte auch Benutzer beinhalten, die zulässige E-Mails mit falsch geschriebenen E-Mail-Adressen schicken oder nicht länger für das Unternehmen arbeiten. Es wird empfohlen, dass der Wert mindestens 2 beträgt.

4. Klicken Sie auf **Test**, um die Einstellungen für Directory Harvesting zu überprüfen. Legen Sie eine interne E-Mail-Adresse fest, und klicken Sie auf **OK**, um zu überprüfen, dass das Active Directory durchsucht werden kann. Wiederholen Sie den Test mit einer nicht existierenden E-Mail-Adresse, um sicherzustellen, dass die Suche im Active Directory fehlschlägt.

5. Klicken Sie auf die Registerkarte **Aktionen** oder **Weitere** um die Aktionen auszuwählen, die bei Spam-Nachrichten durchgeführt werden sollen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails in diesem Handbuch.

HINWEIS: Wenn die Option Directory Harvesting auf SMTP Protocol Sink eingestellt ist, wird nur die Option **Häufigkeit in dieser Datei protokollieren** auf der Registerkarte **Aktionen** angezeigt.

Phase 2 - Auswahl des Verfahrens für Directory Harvesting

1. Klicken Sie auf **Antispam ► Filterpriorität ► Eigenschaften** und dann auf den Knoten **SMTP-Übertragungsfilter**.

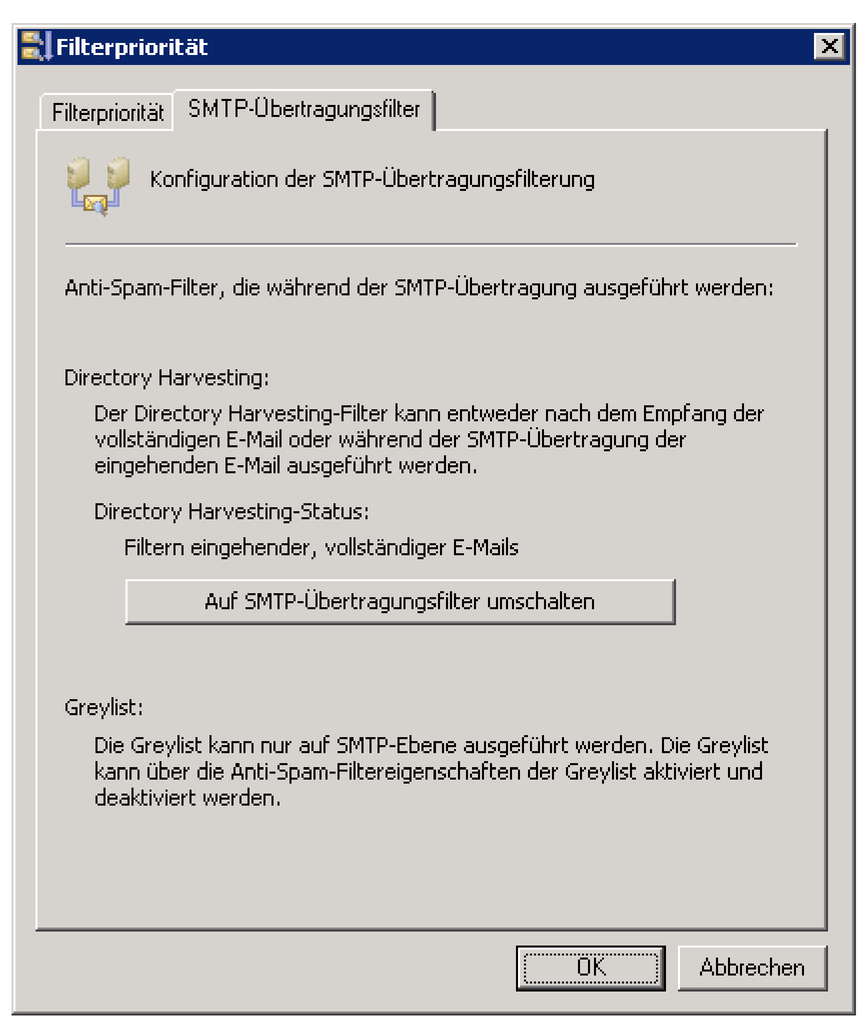


Bild 24 - Der Dialog "Anti-Spam-Reihenfolge"

2. Klicken Sie auf die Schaltfläche, um zwischen folgenden Optionen umzuschalten:

- **Vollständige E-Mail-Filterung** - Die Filterung erfolgt, wenn die gesamte E-Mail empfangen ist.
- **SMTP-Übertragungsfilter** - Die Filterung erfolgt während der SMTP-Übertragung, indem geprüft wird, ob die E-Mail-Empfänger existieren, bevor der Nachrichtentext und die Anhänge empfangen werden.

  HINWEIS: Wenn Sie diese Option auswählen, wird die Option "Directory Harvesting" immer vor anderen Spamfiltern gestartet.

3. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

E-Mail-Blocklist

Die E-Mail-Blocklist ist eine Datenbank der E-Mail-Adressen und Domänen, von denen Sie niemals E-Mails empfangen wollen.

Dieser Filter ist standardmäßig nach Installation von GFI MailEssentials aktiviert.

Konfiguration Email Blocklist

Klicken Sie auf **Anti-Spam** ► **Anti-Spam-Filter** ► **E-Mail-Blocklist** ► **Eigenschaften.**

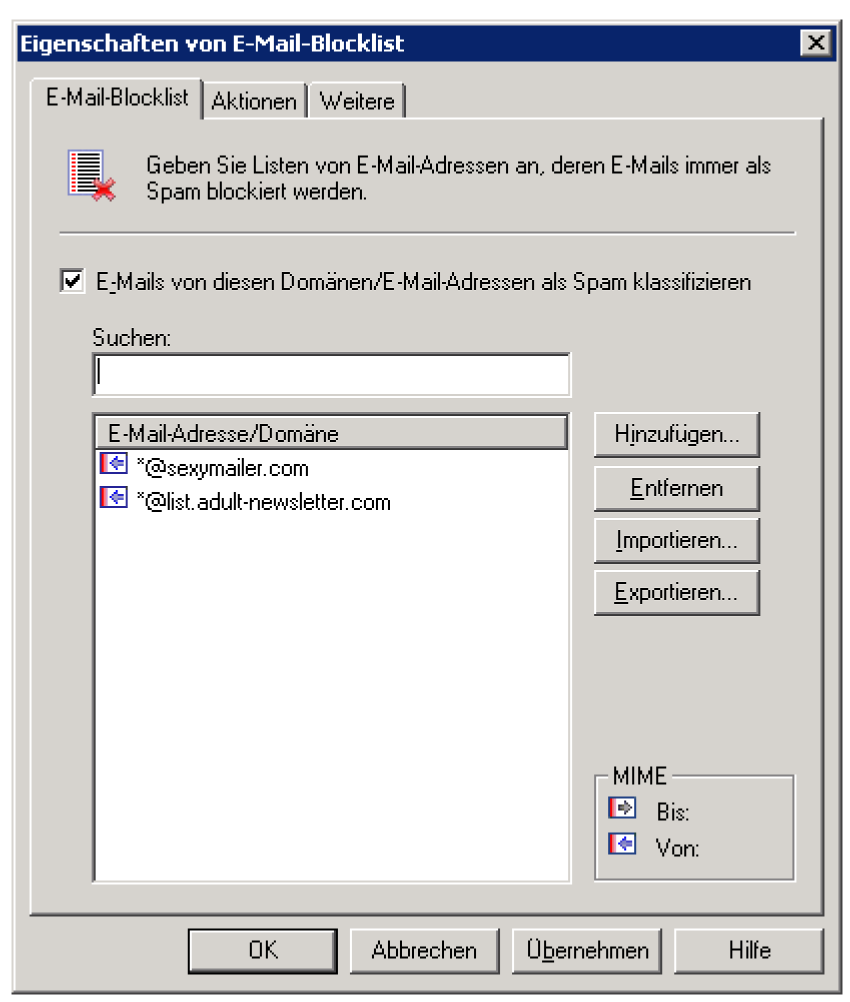


Bild 25 - Die E-Mail-Blocklist

2. Konfigurieren Sie auf der Registerkarte **E-Mail-Blocklist** die E-Mail-Adressen und Domänen, die blockiert werden sollen.

OPTION	BESCHREIBUNG
E-Mails von diesen Domänen/E-Mail-Adressen als Spam klassifizieren	Aktivieren/Deaktivieren Sie diese Option, um die E-Mail-Blocklist zu aktivieren/deaktivieren.
Hinzufügen	Fügen Sie E-Mail-Adressen, E-Mail-Domänen oder komplette Domänen-Suffixe zur Blocklist für hinzu. 1. Geben Sie die E-Mail-Adresse, Domäne (z. B. *@spammer.com) oder das vollständige Domänensuffix (z. B. *@*.tv) ein, die der Blocklist hinzugefügt werden sollen. 2. Geben Sie den E-Mail-Header im entsprechenden Feld an, um die jeweiligen E-Mails der Blocklist hinzuzufügen. **HINWEIS:** Weitere Informationen zum Unterschied zwischen SMTP und MIME finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID002678 3. (Optional) Sie können auch dem Eintrag im Feld **Beschreibung** eine Beschreibung hinzufügen.
Entfernen	Wählen Sie einen Blocklist-Eintrag aus, und klicken Sie auf **Entfernen**, um zu löschen.

Option	Beschreibung
Importieren	Importieren Sie eine Liste von Blocklist-Einträgen aus einer XML-Datei. **HINWEIS:** Eine Liste mit Einträgen kann aus einer XML-Datei importiert werden, die dieselbe Struktur wie Exporte von Listeneinträgen in GFI MailEssentials aufweist.
Exportieren	Exportieren Sie eine Liste von Blocklist-Einträgen in eine XML-Datei.
Suchen	Geben Sie einen Eintrag ein, nach dem gesucht werden soll. Übereinstimmende Einträge werden aus den Blocklist-Einträgen herausgefiltert.

3. Klicken Sie auf die Registerkarte **Aktionen** bzw. **Weitere** um die Aktionen für Spam-Nachrichten auszuwählen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen in diesem Handbuch.

4. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

IP-DNS-Blocklist

GFI MailEssentials unterstützt verschiedene IP-DNS-Blocklist. Diese SMTP-Server-Datenbanken enthalten Listen von Servern, die für Spam-Aktionen verwendet wurden. Es gibt verschiedene IP-DNS-Blocklist von Drittanbietern, die sehr zuverlässig sein können, weil sie klar definierte Prozeduren für die Aufnahme und Aussonderung aus der IP-DNS-Blocklist verwenden, aber auch weniger zuverlässige Listen. GFI MailEssentials vergleicht die IP-Adresse, die mit dem Perimeter-SMTP-Server verbunden ist, mit der IP-DNS-Blocklist.

GFI MailEssentials speichert alle geprüften IP-Adressen in einer internen Datenbank und führt für die gleichen IP-Adressen mit der IP-DNS-Blocklist keine weiteren Prüfungen durch. Die IP-Adressen werden vier Tage lang in der Datenbank gehalten bzw. bis das SMTP-Protokoll neu gestartet wird.

Dieser Filter ist standardmäßig nach Installation von GFI MailEssentials aktiviert.

Wichtige Hinweise

1. Der DNS-Server muss korrekt konfiguriert sein, damit diese Funktion zur Verfügung steht. Ist dies nicht der Fall, kommt es zu einem Zeitüberlauf, und der E-Mail-Traffic wird verzögert. Weitere Informationen dazu finden Sie unter **http://kbase.gfi.com/showarticle.asp?id=KBID001770**.

2. Die Abfrage einer IP-DNS-Blocklist kann eine gewisse Zeit erfordern (je nach Ihrer Verbindung), sodass E-Mails etwas verzögert werden, insbesondere wenn mehrere IP-DNS-Blocklist abgefragt werden.

3. Stellen Sie sicher, dass alle Perimeter-SMTP-Server im entsprechenden Dialog festgelegt wurden, die von der Filterung der IP-DNS-Blocklist ausgeschlossen werden sollen. Weitere Informationen finden Sie unter SMTP-Servereinstellungen.

Konfiguration der IP-DNS-Blocklist

1. Klicken Sie auf **Anti-Spam ► Anti-Spam-Filter ► IP-DNS-Blocklist ► Eigenschaften**.

2. Aktivieren Sie das Kontrollkästchen **Mail-Server auf Eintrag in einer der folgenden IP-DNS-Blocklist überprüfen:**

3. Wählen Sie die entsprechenden IP-DNS-Blocklist aus um eingehende E-Mails zu prüfen und klicken Sie auf die Schaltfläche **Testen** um zu kontrollieren, ob die ausgewählten Blocklisten verfügbar sind.

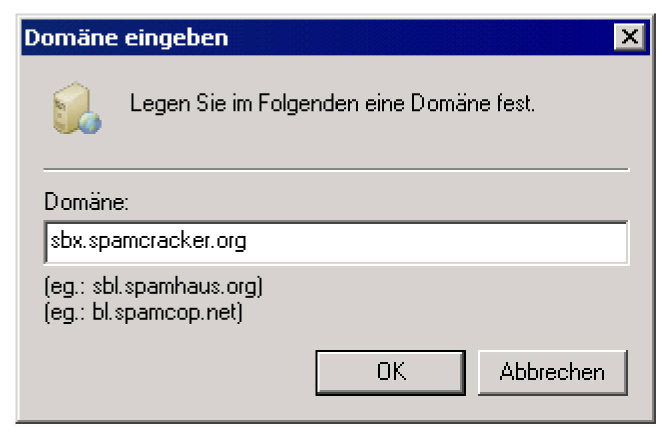


Bild 26 - Hinzufügen weiterer IP-DNS-Blocklist

4. Bei Bedarf können Sie weitere IP-DNS-Blocklist zu den bereits in der Liste aufgeführten hinzufügen, indem Sie auf die Schaltfläche **Hinzufügen** klicken und die Domäne mit der IP-DNS-Blocklist eingeben.

HINWEIS: Die Referenzreihenfolge für eine aktivierte IP-DNS-Blocklist können Sie ändern, indem Sie eine Blockliste auswählen und dann auf die Schaltflächen **Aufwärts** bzw. **Abwärts** klicken.

5. Wählen Sie die Option **E-Mails von dynamischen IP-Adressen in SORBS.net blockieren** aus, damit GFI MailEssentials Spam-Mails von Botnet/Zombies erkennen kann. Dazu vergleicht GFI MailEssentials die eingehende Verbindungs-IP mit bekannten Botnet-/Zombie-IP-Adressen in der Sorbs.net-Datenbank.

6. Klicken Sie auf **Übernehmen** um die Konfiguration zu speichern.

7. Klicken Sie auf die Registerkarte **Aktionen** oder **Weitere** um die Aktionen auszuwählen, die bei Spam-Nachrichten durchgeführt werden sollen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt **Spam-Aktionen - Umgang mit Spam-Mails** in diesem Handbuch.

8. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

URI-DNS-Blocklist

Ein Uniform Resource Identifier (URI) ist ein Standard für den Zugriff auf Ressourcen im Web. Übliche URIs wie die URLs (Web-Adressen) und Uniform Resource Names (URNs) dienen zur Identifizierung des Ziels für Hypertext-Links sowie der Quellen von Bildern, Daten und anderen Objekten auf einer Website. URLs werden häufig bei Websites verwendet, können aber auch Teil einer E-Mail-Nachricht sein.

URI-DNS-Blocklist unterscheiden sich von den meisten anderen RBLs dadurch, dass mit ihnen Spam-Mails anhand der URIs in der Textnachricht erkannt werden können. Im Gegensatz zu den meisten anderen RBLs werden URI-DNS-Blocklist nicht verwendet um Spam-Absender zu blockieren. Stattdessen können sie Nachrichten blockieren, in deren Text Spam-Hosts, beispielsweise Web-Server, Domänen und Websites, enthalten sind.

Dieser Filter ist standardmäßig nach Installation von GFI MailEssentials aktiviert.

Konfiguration der URI-DNS-Blocklist

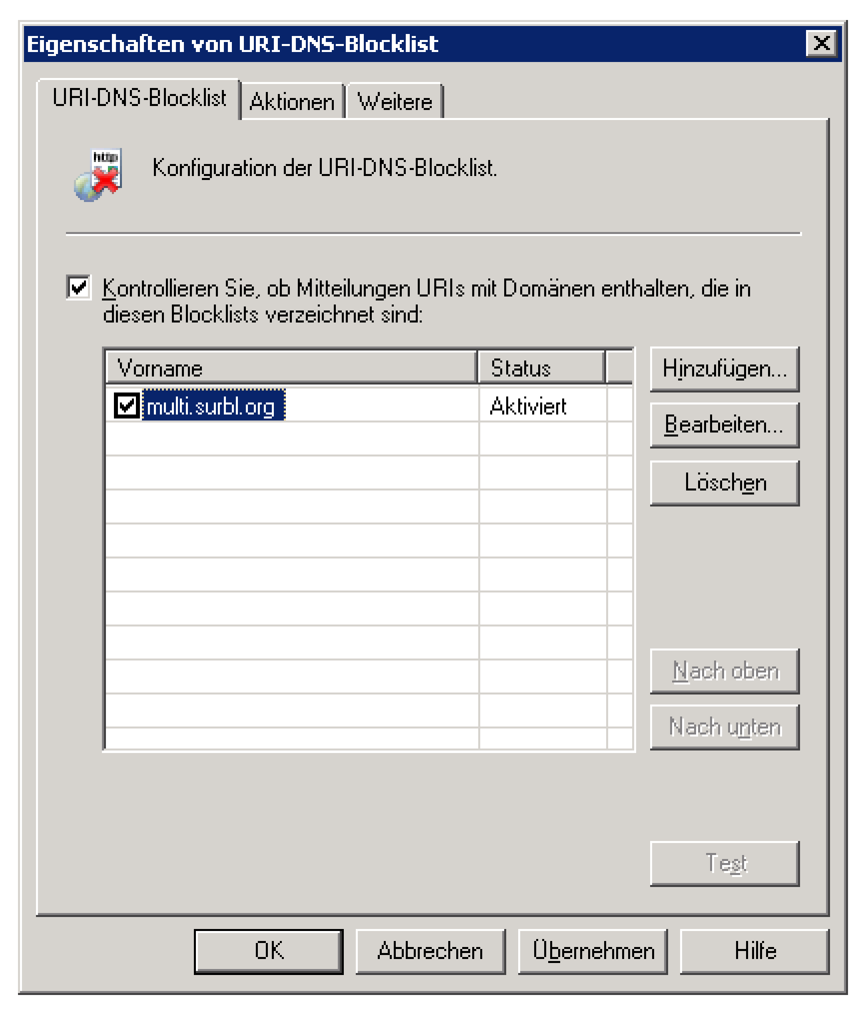


Bild 27 - URI-DNS-Blocklist - Eigenschaften

1. Klicken Sie auf **Anti-Spam** ► **Anti-Spam-Filter** ► **URI-DNS-Blocklist** ► **Eigenschaften**.

2. Klicken Sie auf die Registerkarte URI-DNS-Blocklist:

» Aktivieren/Deaktivieren Sie die Option **Nachricht auf URIs mit Domänen folgender Blocklisten prüfen:** um diese Funktion zu aktivieren/deaktivieren.

» Wählen Sie aus der verfügbaren Liste die Blocklisten aus, die als Referenz verwendet werden sollen, wenn Sie Nachrichten mit der URI-DNS-Blocklist -Funktion URI-DNS-Blocklist prüfen.

» Klicken Sie auf die Schaltfläche **Hinzufügen** um weitere URI-DNS-Blocklist hinzuzufügen.

3. Testen Sie die Verbindung durch Klicken auf die Schaltfläche **Testen** und klicken Sie auf **Übernehmen** um die Einstellungen zu speichern.

HINWEIS 1: Definieren Sie den vollständigen Namen der Domäne (beispielsweise URIBL.com) mit der Blockliste.

HINWEIS 2: Deaktivieren Sie alle anderen URI-DNS-Blocklist, wenn Sie multi.surbl.org aktivieren, da sonst die E-Mail-Bearbeitungszeit verlängert wird.

4. Klicken Sie auf die Registerkarte **Aktionen** oder **Weitere** um die Aktionen auszuwählen, die bei Spam-Nachrichten durchgeführt werden sollen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt **Spam-Aktionen - Umgang mit Spam-Mails** in diesem Handbuch.

5. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

Sender Policy Framework (SPF)

Der SPF-Filter basiert auf dem Community-Konzept, wobei die Absender ihre Mail-Server in einem SPF-Datensatz mitteilen. Dieser Filter erkennt gefälschte Absender.

» **Beispiel:** Wird eine E-Mail von xyz@companyABC.com gesendet, muss companyABC.com einen SPF-Datensatz veröffentlichen, damit der SPF-Filter erkennen kann, ob die E-Mail tatsächlich über das Netzwerk von companyABC.com versendet wurde oder der Absender gefälscht ist. Wenn kein SPF-Datensatz durch CompanyABC.com veröffentlicht wurde, meldet SPF als Ergebnis 'unknown'.

Weitere Informationen über SPF und dessen Funktionen finden Sie auf der Sender Policy Framework Site unter: **http://www.openspf.org**.

Der SPF-Filter ist standardmäßig NICHT aktiviert und sollte nur aktiviert werden, wenn Sie glauben, dass die Gefahr gefälschter Absender hoch ist.

GFI MailEssentials verlangt nicht die Veröffentlichung von SPF-Datensätzen. Nutzen Sie zur Veröffentlichung von SPF-Datensätzen den SPF-Assistenten unter:

http://www.openspf.org/wizard.html.

Voraussetzungen

Führen Sie folgende Schritte aus, bevor Sie den SPF-Filter bei einer Serverinstallation ohne Gateway aktivieren:

1. Klicken Sie mit der rechten Maustaste auf **Anti-Spam ► Anti-Spam-Filter ► Eigenschaften** und dann auf die Registerkarte **Perimeter SMTP-Server**.

2. Klicken Sie auf die Schaltfläche **Automatisch erkennen** in der Setup-Option für Perimeter SMTP, eine DNS-MX-Suche durchzuführen und automatisch die IP-Adresse Ihres Perimeter SMTP-Servers zu definieren.

Konfiguration des SPF

1. Wählen Sie: **Anti-Spam ► Anti-Spam-Filter ► Sender Policy Framework ► Eigenschaften.**

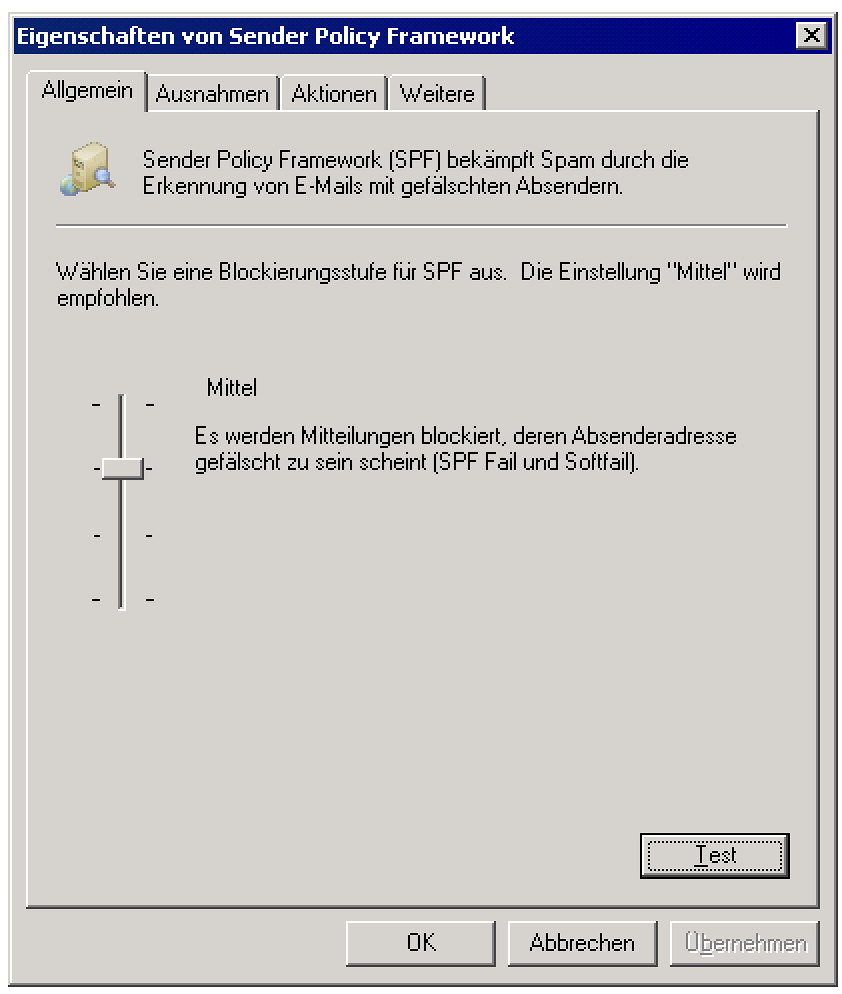


Bild 28 - Konfiguration der SPF-Blockebene

2. Definieren Sie die Empfindlichkeit des SPF-Tests mit dem Schieberegler und klicken Sie auf

Übernehmen. Wählen Sie eine der vier Ebenen:

- **Keine**: Keine Nachrichten blockieren SPF-Tests werden ignoriert.
- **Niedrig:** Nur Nachrichten blockieren, deren Absender als gefälscht erkannt wurde. Diese Option behandelt alle Nachrichten mit gefälschten Absendern als Spam.
- **Mittel**: Alle Nachrichten blockieren, die anscheinend einen gefälschten Absender haben. Diese Option behandelt alle Nachrichten als Spam-Mails, die anscheinend von einem gefälschten Absender stammen.

  HINWEIS: Dies ist die Standardeinstellung und empfohlene Einstellung.
- **Hoch:** Alle Nachrichten blockieren, deren Absender nicht nachweislich korrekt ist. Diese Option behandelt alle E-Mails als Spam, sofern nicht nachgewiesen werden kann, dass der Absender nicht gefälscht ist.

  HINWEIS: Da die meisten E-Mail-Server keinen SPF-Datensatz unterstützen, wird diese Option nicht empfohlen.

3. Testen Sie die DNS-Einstellungen/Dienste, indem Sie auf **Testen** klicken.

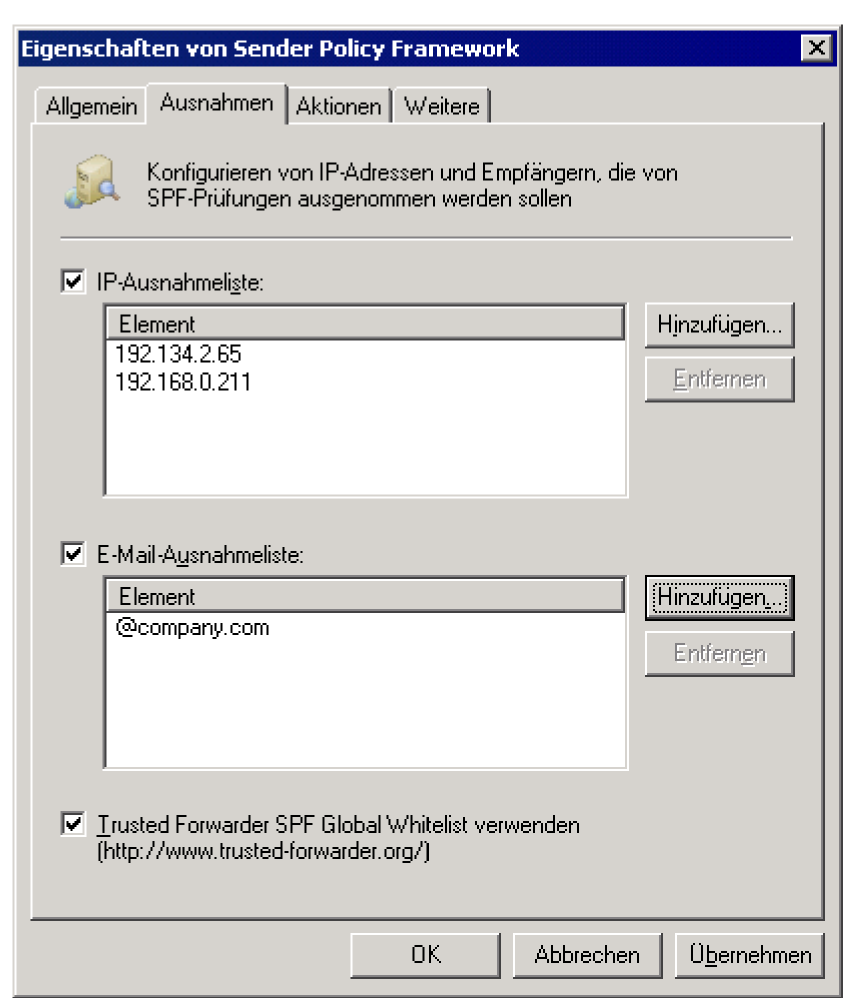


Bild 29 - Konfiguration der SPF-Ausnahmen

4. Klicken Sie auf die Registerkarte **Ausnahmen** um die IP-Adressen und Empfänger zu konfigurieren, die bei den SPF-Prüfungen ausgeschlossen werden sollen:

- **IP-Ausnahmeliste:** Einträge in dieser Liste werden bei den SPF-Prüfungen automatisch übersprungen. Klicken Sie auf **Hinzufügen** um eine neue IP-Adresse hinzuzufügen, oder wählen Sie Einträge aus der Liste aus und klicken Sie auf die Schaltfläche **Entfernen** um die markierten Einträge zu entfernen. Deaktivieren Sie das Kontrollkästchen IP-Ausnahmeliste, wenn Sie die **IP-Ausnahmeliste** nicht verwenden wollen.

  HINWEIS: Beim Hinzufügen von IP-Adressen zur IP-Ausnahmeliste können Sie auch einen Bereich von IP-Adressen in CIDR-Notation eingeben.

- **E-Mail-Ausnahmeliste:** Mit dieser Option wird sichergestellt, dass bestimmte Absender oder Empfänger von E-Mails von SPF-Prüfungen ausgenommen werden; dies gilt auch für abgelehnte Nachrichten. E-Mail-Adressen können wie folgt eingegeben werden:
  - localpart - 'abuse' (Treffer sind 'abuse@abc.com', 'abuse@xyz.com', usw...)
  - Domäne - '@abc.com' (Treffer sind 'john@abc.com', 'jill@abc.com' usw.....)
  - komplett - 'joe@abc.com' (Treffer ist nur 'joe@abc.com')
- Globale Trusted Forwarder SPF-Whitelist: http://www.trusted-forwarder.org/Diese Whitelist (www.trusted-forwarder.org) enthält eine globale Whitelist für SPF-Benutzer. Auf diese Weise werden zulässige E-Mails erlaubt, die über bekannte vertrauenswürdige E-Mail-Versender versendet wurden.

  HINWEIS: Standardmäßig ist diese Einstellung aktiviert. Wir empfehlen, diese Option immer aktiviert zu lassen.

5. Klicken Sie auf die Registerkarte **Aktionen** oder **Weitere** um die Aktionen für als Phishing-E-Mails identifizierte Nachrichten auszuwählen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails in diesem Handbuch.

6. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

Greylist

Der Greylist-Filter blockiert temporär eingehende E-Mails von unbekannten Absendern, und schickt eine Nachricht zum wiederholten Senden. Dies erfolgt, da ein nicht RFC-konformer SMTP-Server versuchen wird, eine E-Mail erneut zu senden, falls eine Nachricht zum wiederholten Senden empfangen wird. Spam-Server ignorieren diese Fehlermeldungen normalerweise. Falls die E-Mail in einem festgelegten Zeitraum erneut empfangen wird, führt die Greylist Folgendes durch:

- Die Daten des Absenders werden in einer Datenbank gespeichert, so dass bei einer erneuten E-Mail von diesem Absender diese nicht auf die Greylist gelangt.
- Die E-Mail wird empfangen und einer Spam-Prüfung unterzogen.

Die Greylist ist standardmäßig DEAKTIVIERT.

Wichtige Hinweise

1. Um die Greylist zu aktivieren, muss GFI MailEssentials auf dem Perimeter-SMTP-Server installiert sein. Weitere Informationen finden Sie unter http://kbase.gfi.com/showarticle.asp?id=KBID003796.

2. Die Greylist enthält Ausnahmelisten, so dass bestimmte E-Mail-Adressen, Domänen und IP-Adressen nicht auf die Greylist gesetzt werden. Ausnahmen können in folgenden Situationen konfiguriert werden:

- E-Mails von bestimmten E-Mail-Adressen, Domänen oder IP-Adressen können nicht verzögert werden.
- E-Mails an einen bestimmten lokalen Benutzer können nicht verzögert werden.
- Der Server eines zulässigen Absenders schickt eine abgelehnte E-Mail nicht zurück.

Konfigurieren der Greylist

1. Wählen Sie **Anti-Spam** ► **Anti-Spam-Filter** ► **Greylist** ► **Eigenschaften**.

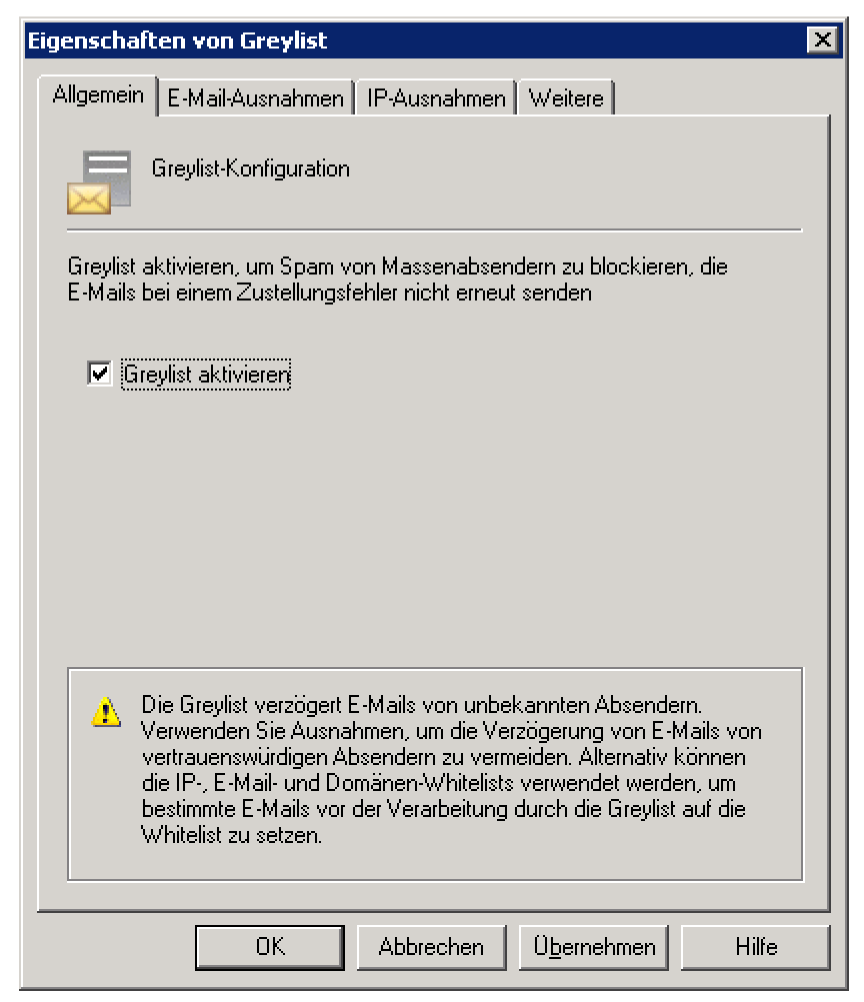


Bild 30 - Greylist

2. Aktivieren/deaktivieren Sie auf der Registerkarte **Allgemein** das Kontrollkästchen **Greylist aktivieren**, um die Greylist zu aktivieren oder zu deaktivieren.

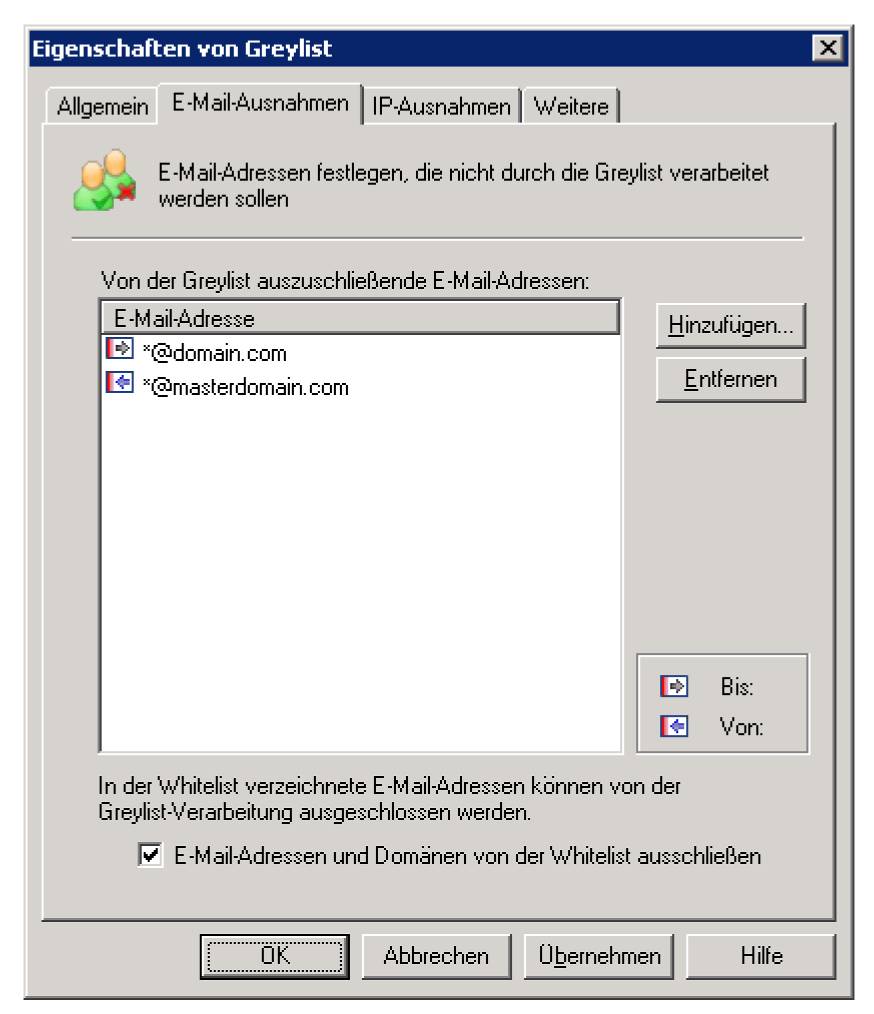


Bild 31 - E-Mail-Ausnahmen

3. Legen Sie auf der Registerkarte **E-Mail-Ausnahmen** die E-Mail-Adressen und Domänen fest, die nicht auf der Greylist erscheinen sollen. Klicken Sie anschließend auf **Hinzu...**.

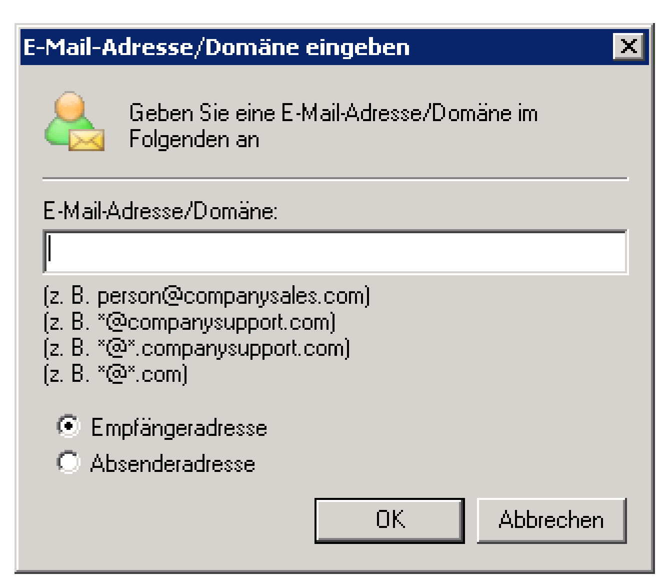


Bild 32 - Hinzufügen von E-Mail-Ausnahmen

4. Legen Sie im Dialog **E-Mail-Adresse/Domäne eingeben** Folgendes fest:

- vollständige E-Mail-Adresse oder
- E-Mails von einer ganzen Domäne (z. B.: *@trusteddomain.com) oder
- eine ganze Top-Level-Domäne (z. B.: *@*.mil oder *@*.edu).

Legen Sie auch fest, ob sich die Ausnahme auf Absender oder lokale Empfänger bezieht.

Beispiel 1: E-Mails nicht auf die Greylist setzen, falls der Empfänger administrator@mydomain.com ist, so dass E-Mails an diese Domäne nie verzögert werden.

Beispiel 2: E-Mails nicht auf die Greylist setzen, falls die Domäne des Absenders trusteddomain.com (*@trusteddomain.com) ist, so dass E-Mails von dieser Domäne nie verzögert werden.

Klicken Sie auf **OK**, um die Ausnahme hinzuzufügen.

5. Um E-Mail-Adressen und Domänen auf der Whitelist von der Greylist und der Verzögerung auszuschließen, wählen Sie **E-Mail-Adressen und Domänen von der Whitelist ausschließen**.

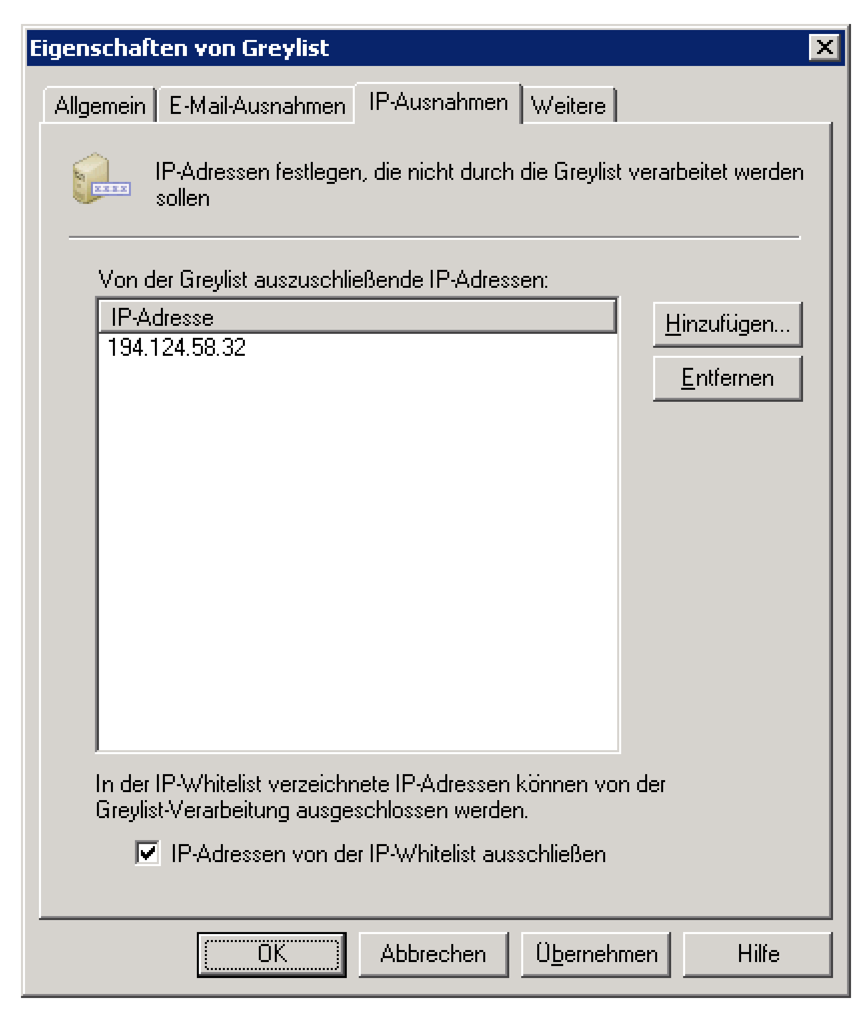


Bild 33 - IP-Adressen-Ausnahmen

6. Wählen Sie die Registerkarte **IP-Ausnahmen**, um IP-Adressen von der Greylist auszuschließen. Klicken Sie auf **Hinzu…**, und legen Sie die auszuschließende IP-Adresse fest.

7. Um IP-Adressen auf der Whitelist von der Greylist und der Verzögerung auszuschließen, wählen Sie **IP-Adressen von der Whitelist ausschließen**.

8. Um Greylist-Ereignisse in einer Protokolldatei zu speichern, wählen Sie auf die Registerkarte **Aktionen** die Option **Ereignis in folgender Datei protokollieren**.

HINWEIS: Protokolldateien können sehr groß werden. GFI MailEssentials verfügt über einen Protokollrotator, durch den regelmäßig neue Protokolldateien erstellt werden, sobald eine Protokolldatei eine bestimmte Größe erreicht. Um den Protokollrotator zu aktivieren, öffnen Sie **Anti-Spam ► Anti-Spam-Einstellungen**. Aktivieren Sie auf der Registerkarte **Protokolldateien** das Kontrollkästchen **Protokollrotator aktivieren**, und legen Sie die Rotationsbedingungen fest.

Header-Kontrolle

Der Filter zur Header-Kontrolle analysiert E-Mail-Header, um zu erkennen, ob es sich um Spam handelt.

Konfiguration der Header-Prüfung

1. Klicken Sie auf **Anti-Spam** ► **Anti-Spam-Filter** ► **Header-Prüfung** ► **Eigenschaften**.

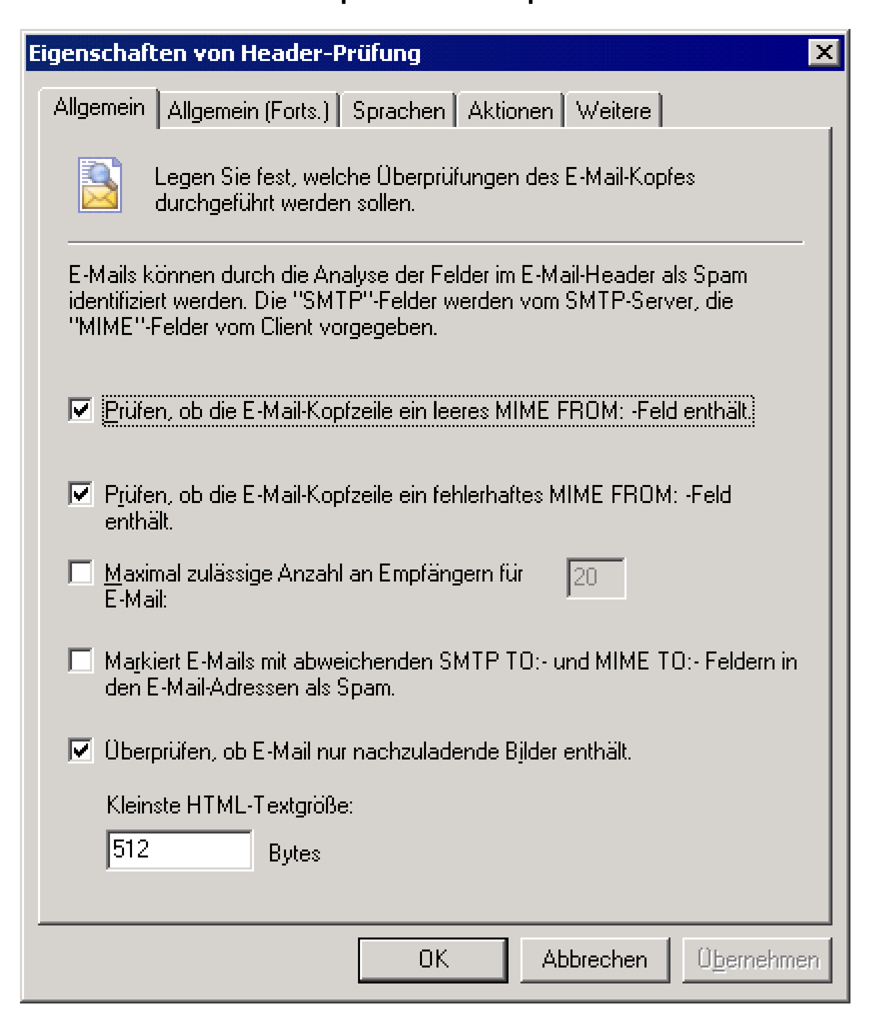


Bild 34 - Registerkarte Header-Prüfung AllgemeinHeader-Prüfung

2. Auf die Registerkarten **Allgemein** und **Allgemein Forts.** können Sie die folgenden Parameter aktiveren, deaktivieren oder konfigurieren.

- **Prüft, ob der E-Mail-Header ein leeres Feld MIME FROM enthält:** Prüft, ob der Absender sich selbst in dem Feld FROM: identifiziert hat. Ist dieses Feld leer, wird die Nachricht als Spam markiert.
- **Prüft, ob der E-Mail-Header ein Feld MIME FROM: enthält:** Der Filter überprüft den MIME-Typ, ob dieser gemäß RFC definiert ist.
- **Maximale Anzahl der zulässigen Empfänger in der E-Mail:** Identifiziert E-Mails mit vielen Empfängern und markiert diese als Spam.
- **Markiert E-Mails mit verschiedenen Feldern SMTP TO: und MIME TO: in den E-Mail-Adressen als Spam:** Überprüft, ob die Felder SMTP TO: und MIME TO: identisch sind. Der E-Mail-Server des Spammers muss immer eine Adresse SMTP TO: enthalten. Die Adresse MIME TO: ist jedoch oft nicht enthalten oder weicht ab.

  HINWEIS: Mit dieser Funktion lassen sich viele Spam-Mails identifizieren, allerdings enthalten auch einige Listen-Server das Feld MIME TO: nicht. Wir empfehlen daher, die Absenderadresse von Newslettern in die Whitelist einzutragen, wenn diese Funktion verwendet werden soll.
- **Überprüfen, ob E-Mail nur nachzuladende Bilder enthält:** Diese Funktion markiert E-Mails als Spam, die nur nachzuladende Bilder und nur minimalen Text enthalten. Diese Funktion identifiziert Spam-Mails, die nur Bilder enthalten.

- **Gültigkeit der Absender-Domäne überprüfen:** Diese Funktion führt eine DNS-Suche in der Domäne durch, die in dem Feld MIME FROM eingetragen ist, und überprüft die Gültigkeit der Domäne.

  HINWEIS: Der DNS-Server muss korrekt konfiguriert sein, damit es nicht zu einem Zeitüberlauf und zu einer Verzögerung der E-Mail-Übertragung kommt. Prüfen Sie Ihren DNS-Server und die Dienste, indem Sie auf **Testen** klicken.

- **Maximal zulässige Anzahl in dem Feld MIME FROM:** Der Filter zur Header-Kontrolle erkennt das Vorhandensein von Zahlen im MIME FROM-Feld. Spammer verwenden oft Tools, die automatisch eine unverwechselbare Antwortadresse erstellen, in der Zahlen verwendet werden.

- **Diese Funktion prüft, ob der E-Mail-Betreff den ersten Teil der Empfänger-E-Mail-Adresse enthält:** Diese Funktion identifiziert personalisierte Spam-Mails, bei denen die Spammer häufig den ersten Teil der Empfänger-E-Mail-Adresse in der Betreffzeile einfügen.

  HINWEIS: Achten Sie darauf, dass Sie E-Mail-Adressen, für die diese Prüfung nicht ausgeführt werden soll, durch einen Klick auf die Schaltfläche **Außer …** konfigurieren. Auf diese Weise werden allgemeine E-Mail-Adressen, an die Kunden antworten, beispielsweise E-Mails von sales@company.com mit einem Betreff 'Ihre E-Mail an den Vertrieb', nicht als Spam markiert

- **E-Mail auf codierte IP-Adressen prüfen:** Überprüft den Nachrichten-Header und den Nachrichtentext auf URLs mit einer im Hexa- oder Oktal-Format codierten IP (http://0072389472/hello.com) oder auf eine Kombination aus Benutzername und Kennwort (beispielsweise: www.citibank.com@scammer.com).
  - Folgende Beispiele würden als Spam gekennzeichnet:
    - *http://12312*
    - *www.microsoft.com:hello%01@123123*

- **E-Mails auf eingebettete GIF-Bilder prüfen:** Prüft, ob die E-Mail mindestens ein eingebettetes GIF-Bild enthält. Eingebettete GIF-Bilder werden oft verwendet um Spam-Filter zu umgehen.

  WICHTIGER HINWEIS: Da einige zulässige E-Mails eingebettete GIF-Bilder enthalten können, liefert diese Option oft falsch-positive Treffer.

- **E-Mail auf Spam-Anhang überprüfen:** Überprüft E-Mail-Anhänge auf Eigenschaften, die bei in Spam-Mails versendeten Dateianhängen häufig sind. Dies ist eines der modernsten Verfahren, das Spammer einsetzen um über Dateianhänge Spam zu versenden.

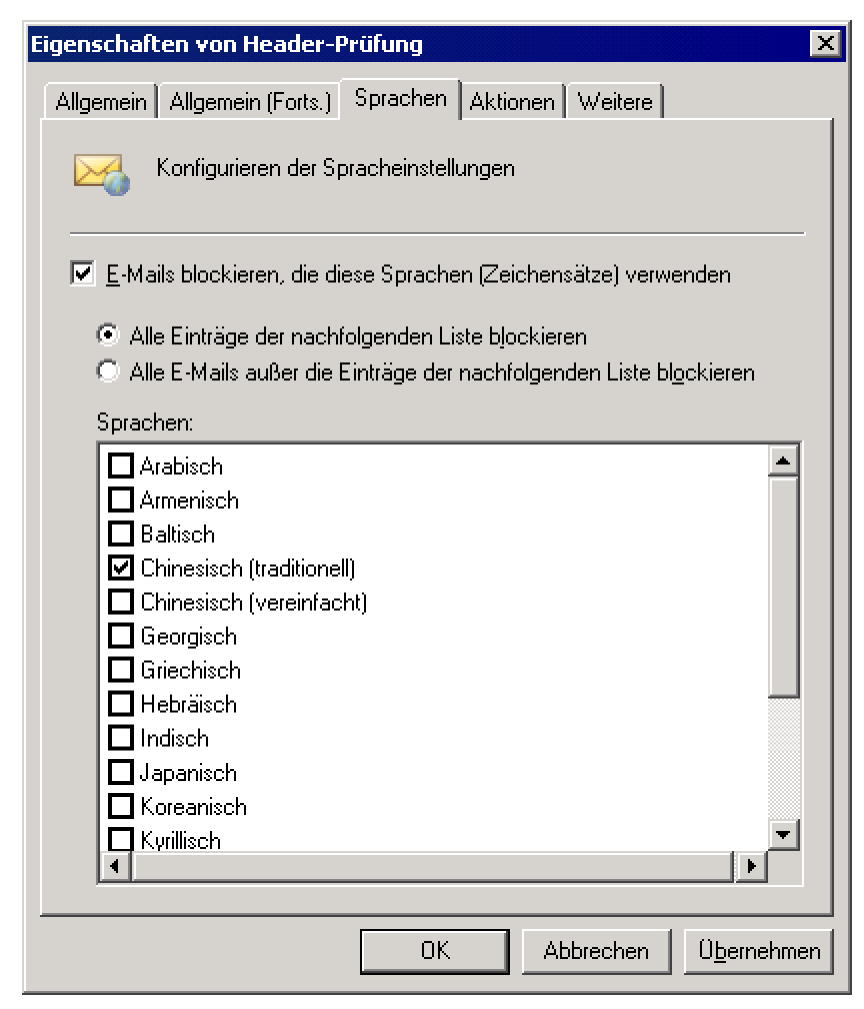


Bild 35 - Spracherkennung

3. Klicken Sie auf der Registerkarte "Sprachen" auf die Option **Mails blockieren, die folgende Sprachen (Zeichensätze) verwenden** um E-Mails zu blockieren, die Zeichensätze verwenden, die für empfangene E-Mails untypisch sind, beispielsweise Chinesisch oder Vietnamesisch.

HINWEIS: Diese Funktion unterscheidet nicht zwischen Sprachen, die den gleichen Zeichensatz verwenden, beispielsweise Italienisch und Französisch.

4. Klicken Sie auf die Registerkarte **Aktionen** oder **Weitere** um die Aktionen auszuwählen, die bei Spam-Nachrichten durchgeführt werden sollen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails in diesem Handbuch.

5. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

Keyword-Prüfung

Keyword-Prüfung erlaubt die Identifizierung von Spam-Mails mit Keywords in den empfangenen E-Mails.

Dieser Filter ist standardmäßig NICHT aktiviert.

Konfiguration der Keyword-Prüfung

1. Klicken Sie auf **Anti-Spam** ▶ **Anti-Spam-Filter** ▶ **Keyword-Prüfung** ▶ **Eigenschaften**.

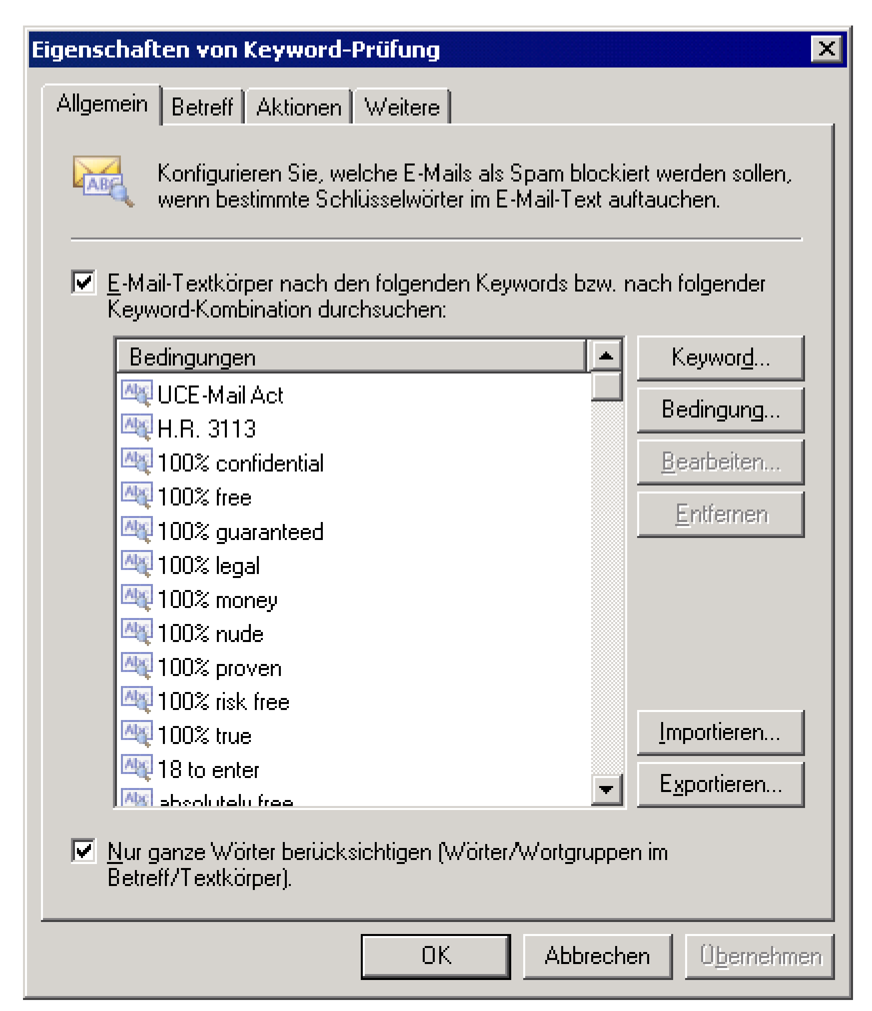


Bild 36 - Anti-Spam-Keyword-Prüfungseigenschaften

2. Aktivieren Sie das Kontrollkästchen **E-Mail-Nachrichtentext auf folgende Keywords oder Keyword-Kombinationen scannen:** um diese Funktion zu aktivieren.

3. Klicken Sie auf die Schaltfläche **Keyword** um Keywords einzugeben. Wenn Sie mehrere Wörter eingeben, interpretiert GFI MailEssentials diese als Phrase.

- **Beispiel:** Bei Eingabe von 'Basketball Sport' sucht GFI MailEssentials nach der Phrase 'Basketball Sport'. Die Regel würde nur aktiviert, wenn diese Phrase gefunden wird, nicht, wenn nur das Wort Basketball oder Sport gefunden wird, aber dazwischen noch weitere Wörter stehen.

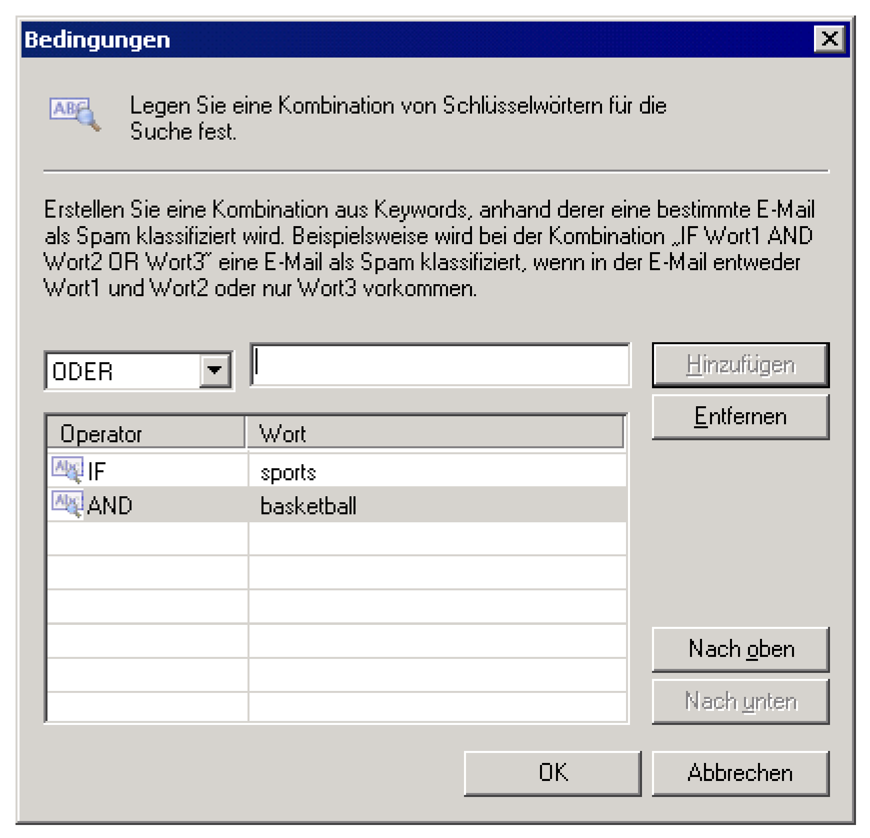


Bild 37 - Hinzufügen einer Bedingung

4. Ergänzen Sie logische Operatoren, indem Sie auf die Schaltfläche **Bedingungen** … klicken.

HINWEIS: Bedingungen sind Kombinationen von Keywords mit den Operanden IF, AND, AND NOT, OR oder OR NOT. Definieren Sie mit Bedingungen Wortkombinationen, die in der E-Mail vorkommen müssen.

- **Beispiel:** Eine Bedingung 'IF Wort1 AND Wort2' prüft, ob Wort1 und Wort2 vorkommen. Beide Wörter müssen in einer E-Mail gefunden sein, damit die betreffende Regel aktiviert wird.

Klicken Sie zum Hinzufügen einer Bedingung auf die Schaltfläche **Bedingungen** …

5. Wählen Sie die Registerkarte Betreff aus und aktivieren Sie das Kontrollkästchen **Die E-Mail-Betreffzeile auf die folgenden Keywords oder Kombinationen von Keywords scannen**. Konfigurieren Sie die Wörter, nach denen in der Betreffzeile der Nachricht gesucht werden soll.

- Klicken Sie zur Eingabe von Einzelwörtern oder Phrasen ohne logische Operatoren auf die Schaltfläche **Keyword** …
- Klicken Sie zur Eingabe von Keywords mit logischen Operatoren auf die Schaltfläche **Bedingungen** …
- Um einen Eintrag hinzuzufügen, wählen Sie den Eintrag aus, und klicken Sie auf **Bearbeiten…**.
- Um einen Eintrag zu löschen, wählen Sie den Eintrag aus, und klicken Sie auf **Entfernen…**.

6. Sie können die Liste mit Schlüsselwörtern im E-Mail-Betreff verwenden, um die Anzeigenamen von Absendern zu filtern. Anzeigenamen von Absendern mit entsprechenden Schlüsselwörtern werden als Spam markiert. Wählen Sie **Liste mit Schlüsselwörtern auch zum Scannen der Anzeigenamen von Absendern verwenden** aus, um diese Option zu aktivieren.

7. Klicken Sie auf die Registerkarte **Aktionen** oder **Weitere** um die Aktionen auszuwählen, die bei Spam-Nachrichten durchgeführt werden sollen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails in diesem Handbuch.

8. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

Bayes'sche Analyse

Der Bayes-Filter ist ein Spam-Filter in GFI MailEssentials, bei dem adaptive Verfahren mit Algorithmen künstlicher Intelligenz genutzt werden um möglichst viele der heute üblichen Spam-Verfahren zu erkennen.

Weitere Informationen über den Bayes-Filter, dessen Konfiguration und Training finden Sie in Anhang - Einsatz des Bayes-Filters in diesem Handbuch.

HINWEIS: Der Bayes-Filter ist standardmäßig deaktiviert.

WICHTIGER HINWEIS: Der Bayes-Filter erreicht seine maximale Leistung frühestens nach einer Woche nach seiner Aktivierung. Diese Zeit ist erforderlich, weil der Bayes-Filter seine Höchsterkennungsrate nur dann erreicht, wenn er sich an Ihre E-Mail-Muster anpasst.

Konfiguration des Bayes-Filters

Die Konfiguration des Bayes-Filters erfordert zwei Phasen:

Phase 1: Konfiguration des Bayes-Filters

Phase 2: Aktivierung des Bayes-Filters

Phase 1: Konfiguration des Bayes-Filters

Der Bayes-Filter Bayes-Filter kann auf zwei Arten trainiert werden:

1. Automatisch durch ausgehende E-Mails.

GFI MailEssentials erfasst zulässige E-Mails (HAM) durch Scannen der ausgehenden E-Mails. Der Bayes-Filter kann aktiviert werden, sobald mindestens 500 ausgehende E-Mails gesammelt wurden (wenn Sie nur englische E-Mails versenden) oder mindestens 1000 ausgehende E-Mails (wenn Sie E-Mails nicht in Englisch versenden).

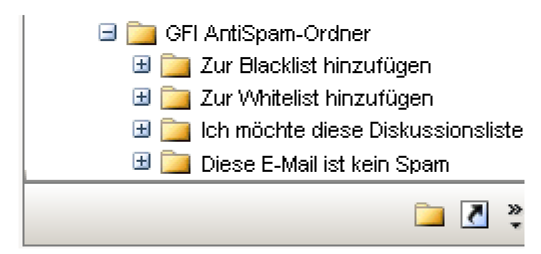


Bild 38 - Training des Bayes-Filters mit zulässigen E-Mails

2. Manuelles Training mit vorhandenen E-Mails

Kopieren Sie 500 bis 1000 E-Mails aus Ihrem Versandordner in den Unterordner **Das sind zulässige E-Mails** in die **Anti-Spam folders** (öffentlichen Ordner) um den Bayes-Filter genauso zu trainieren wie beim Versand von E-Mails.

Phase 2: Aktivierung des Bayes-Filters

Sobald der Bayes-Filter trainiert ist, muss er aktiviert werden.

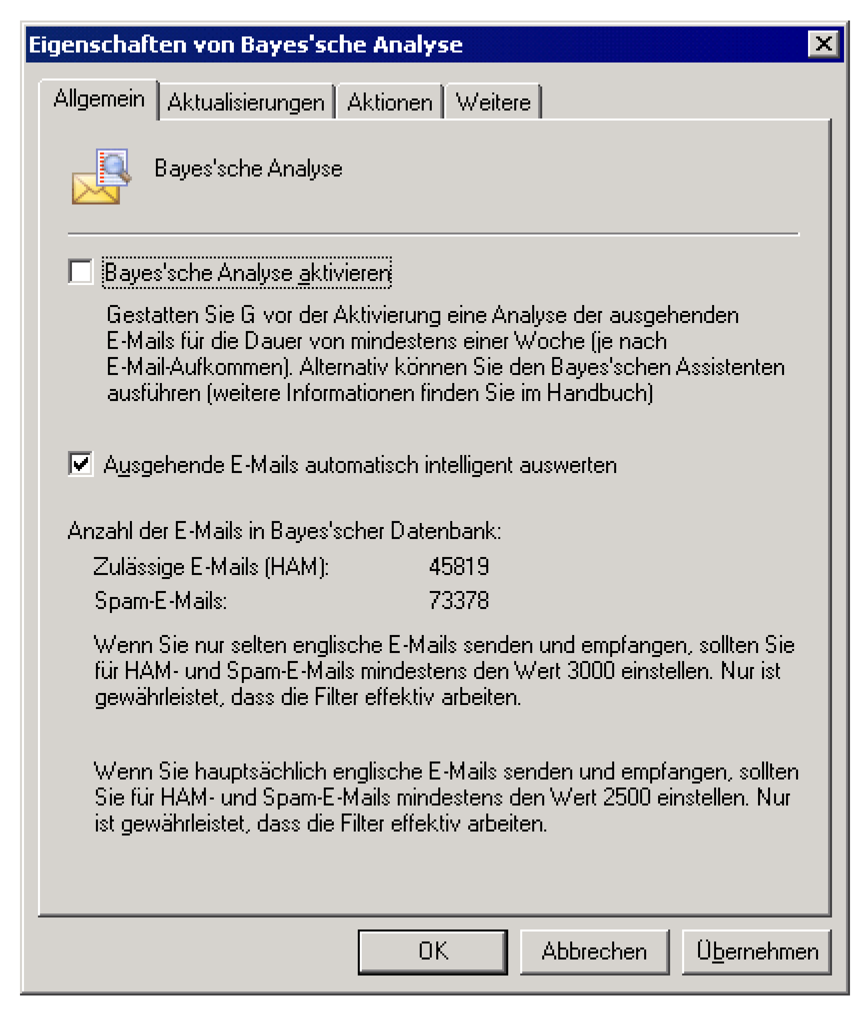


Bild 39 - Bayes-Filter-Analyseeigenschaften

1. Klicken Sie in der Konfigurationskonsole von GFI MailEssentials auf **Anti-Spam ► Anti-Spam-Filter ► Bayes'sche Analyse ► Eigenschaften.** Klicken Sie auf der Registerkarte **Allgemein** auf das Kontrollkästchen Bayes-Analyse aktivieren.

2. Achten Sie darauf, dass die Option **Ausgehende E-Mails automatisch intelligent auswerten** aktiviert ist. Damit wird die Datenbank zulässiger E-Mails zulässige E-Mails laufend mit den Daten ausgehender E-Mails aktualisiert.

3. Konfigurieren Sie auf der Registerkarte **Aktualisierungen** die Häufigkeit der Aktualisierungen für die Spam-Datenbank, indem Sie die Option **Automatische Prüfung auf Updates alle** aktivieren und ein Intervall in Stunden angeben.

HINWEIS 1: Klicken Sie auf die Schaltfläche **Aktualisierungen jetzt herunterladen** um sofort Aktualisierungen herunterzuladen.

HINWEIS 2: Weitere Informationen zur Auswahl der bevorzugten Server sowie zum Herunterladen von Updates mit einem Proxyserver finden Sie unter Automatischer Updates in diesem Handbuch

4. Klicken Sie auf die Registerkarte **Aktionen** oder **Weitere** um die Aktionen auszuwählen, die bei Spam-Nachrichten durchgeführt werden sollen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails in diesem Handbuch.

5. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

Whitelist

Die Whitelist enthält Kriterienlisten, die zulässige E-Mails erkennen. E-Mails, die diesen Kriterien entsprechen, werden nicht von Anti-Spam-Filtern geprüft und immer direkt dem Empfänger zugestellt. E-Mails können mithilfe folgender Kriterien auf die Whitelist gesetzt werden:

- E-Mail-Adresse, E-Mail-Domäne oder IP-Adresse des Absenders
- Absender, an die zuvor eine E-Mail gesendet wurde (Auto-Whitelist)

» Empfänger (lokale E-Mail-Adressen von der Filterung ausschließen)

» Schlüsselwörter im E-Mail-Text oder -Betreff

Die Whitelist und Auto-Whitelist sind standardmäßig aktiviert.

Wichtige Hinweise

1. Das Verwenden der Auto-Whitelist wird dringend empfohlen, weil dadurch ein hoher Prozentsatz an falsch-positiven Ergebnissen eliminiert wird.

2. Fügen Sie zur Stichwort-Whitelist Begriffe hinzu, die von Spammern nicht verwendet werden und die sich auf Ihr Unternehmen beziehen, z. B. Produktnamen. Durch Eingabe zu vieler Stichwörter erhöht sicht die Möglichkeit, dass einige E-Mails nicht von GFI MailEssentials gefiltert und an die Benutzerpostfächer zugestellt werden.

Konfigurieren der Whitelist

1. Wählen Sie **Anti-Spam** ► **Whitelist** ► **Eigenschaften**.

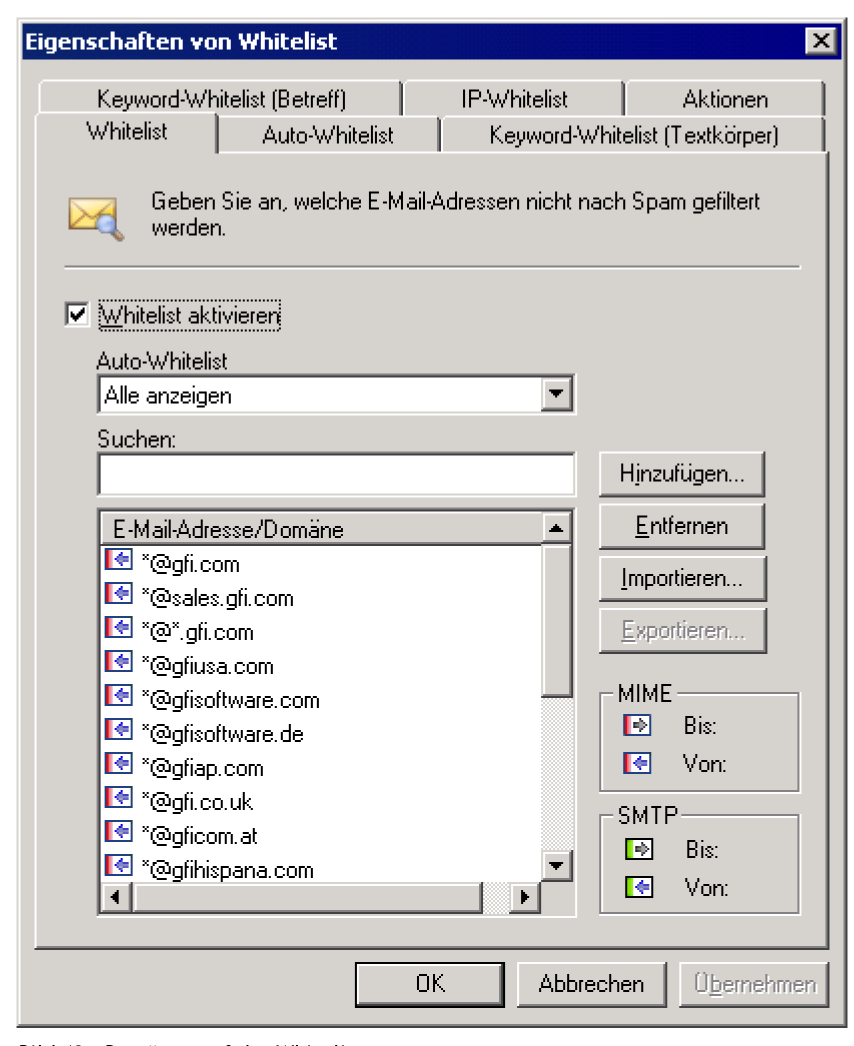


Bild 40 - Domänen auf der Whitelist

2. Legen Sie auf der Registerkarte **Whitelist** die E-Mail-Adressen und Domänen fest, die auf der Whitelist stehen sollen. Aktivieren / deaktivieren Sie die Option **E-Mail-Whitelist aktivieren**, um die Whiteliste zu aktivieren / zu deaktivieren. Konfigurieren Sie die folgenden Whitelist-Optionen:

» **Hinzufügen** - Fügen Sie der Whitelist manuell E-Mail-Adressen, E-Mail-Domänen (z. B. *@companysupport.com) oder komplette Domänen-Suffixe (z. B. *@*.edu) hinzu. Sie können auch den E-Mail-Header im entsprechenden Feld festlegen, um die jeweiligen E-Mails der Whitelist hinzuzufügen. Außerdem können Sie dem Eintrag im Feld **Beschreibung** eine Beschreibung hinzufügen.

HINWEIS: Weitere Informationen zum Unterschied zwischen SMTP und MIME finden Sie unter:

http://kbase.gfi.com/showarticle.asp?id=KBID002678

- **Entfernen** - Wählen Sie einen Whitelist-Eintrag, und klicken Sie auf **Entfernen**, um zu löschen.
- **Importieren** - Importieren Sie eine Liste von Whitelist-Einträgen aus einer XML-Datei.

  HINWEIS: Eine Liste mit Einträgen kann aus einer XML-Datei importiert werden, die dieselbe Struktur wie Exporte von Listeneinträgen in GFI MailEssentials aufweist.
- **Exportieren** - Exportieren Sie eine Liste von -Einträgen in eine XML-Datei.
- **Whitelist-Einträge filtern** - Wählen Sie ein Element aus der Dropdown-Liste aus, um die Einträge anhand folgender Kriterien zu filtern:
  - **Alle anzeigen** - Zeigt alle Einträge in der Whitelist an
  - **Manuelle Eingaben anzeigen** - Zeigt manuell hinzugefügte Einträge an
  - **Automatische Eingaben zeigen** - Zeigt Einträge an, die mit der Funktion Auto-Whitelist hinzugefügt wurden
  - **Einträge pro Domäne insgesamt** -Zeigt eine Liste der Domänen in der Whitelist sowie die Anzahl der Einträge an, die mit dieser Domäne verknüpft sind.
- **Suche** - Geben Sie einen Eintrag ein, nach dem gesucht werden soll. Übereinstimmende Einträge werden aus den Whitelist-Einträgen herausgefiltert.

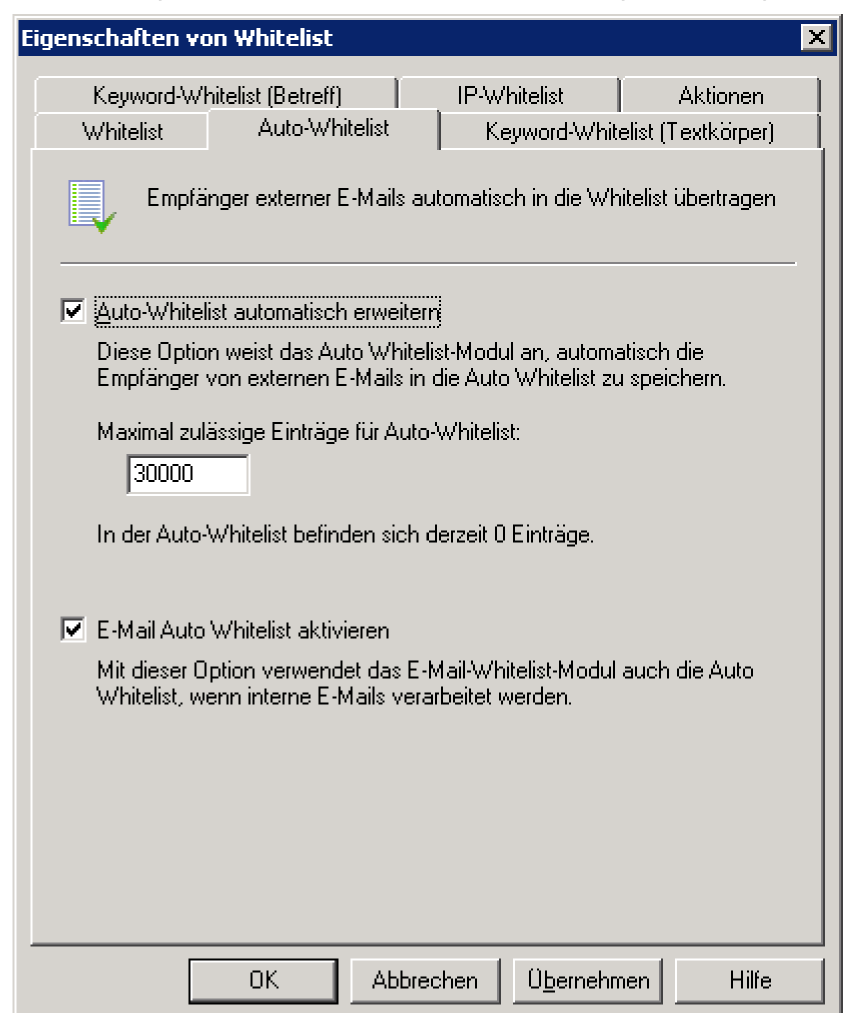


Bild 41 - Optionen für die automatische Whitelist

5. Klicken Sie auf die Registerkarte **Automatische Whitelist**, um die folgenden Optionen für die automatische Whitelist zu konfigurieren:

- **Automatische Whitelist automatisch füllen:** Wenn Sie diese Option wählen, werden die Empfängeradressen abgehender E-Mails automatisch in die Whitelist eingetragen.
- **Maximal zulässige Einträge für Auto-Whitelist:** Geben Sie an, wie viele Einträge die Auto-Whitelist maximal enthalten darf. Sobald dieses Limit überschritten wird, werden die ältesten und am wenigsten verwendeten Einträge automatisch durch neue Einträge ersetzt.

  HINWEIS: Ein Wert, der größer als 30.000 ist, kann sich negativ auf die Leistung von GFI MailEssentials auswirken.
- **E-Mail-Auto-Whitelist aktivieren:** Bei Auswahl dieser Option wird überprüft, ob der Absender einer eingehenden E-Mail in der Liste der Auto-Whitelist verzeichnet ist. Ist dies der Fall, wird die E-Mail direkt an das Postfach des Empfängers weitergeleitet.

HINWEIS: Einträge in der automatischen Whitelist können Sie in der Registerkarte **Whitelist** anzeigen, wenn Sie auf die Option "Automatische Einträge anzeigen" in dem Dropdown-Feld **Whitelist-Einträge filtern** klicken.

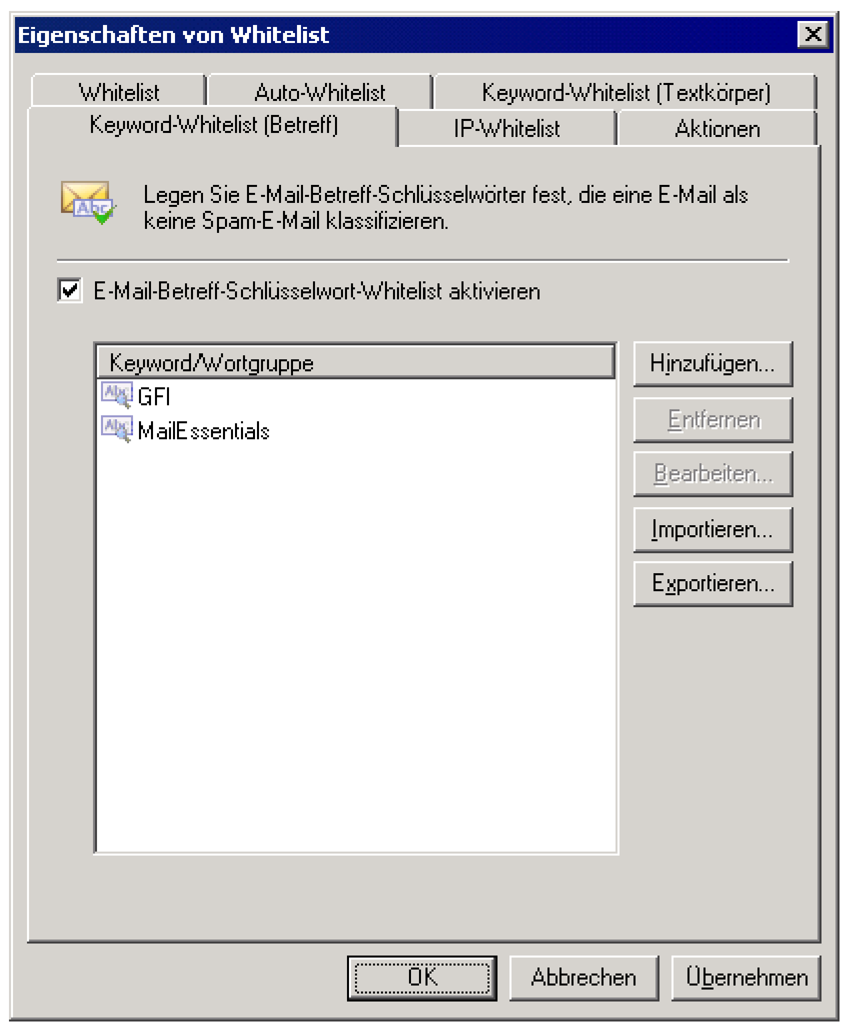


Bild 42 - Whitelist-Keywords

6. Klicken Sie auf die Registerkarte **Keyword-Whitelist** (Betreff) oder Keyword-Whitelist (Nachrichtentext) um die Keywords anzugeben, die E-Mails als HAM (zulässige E-Mail) markieren, sodass die E-Mail automatisch von den Spam-Filtern ignoriert wird. Definieren Sie neue Keywords, indem Sie auf die Schaltfläche **Hinzufügen** klicken oder mit den Schaltflächen **Entfernen**, **Bearbeiten**, **Importieren** und **Exportieren** die vorhandenen Keywords verändern.

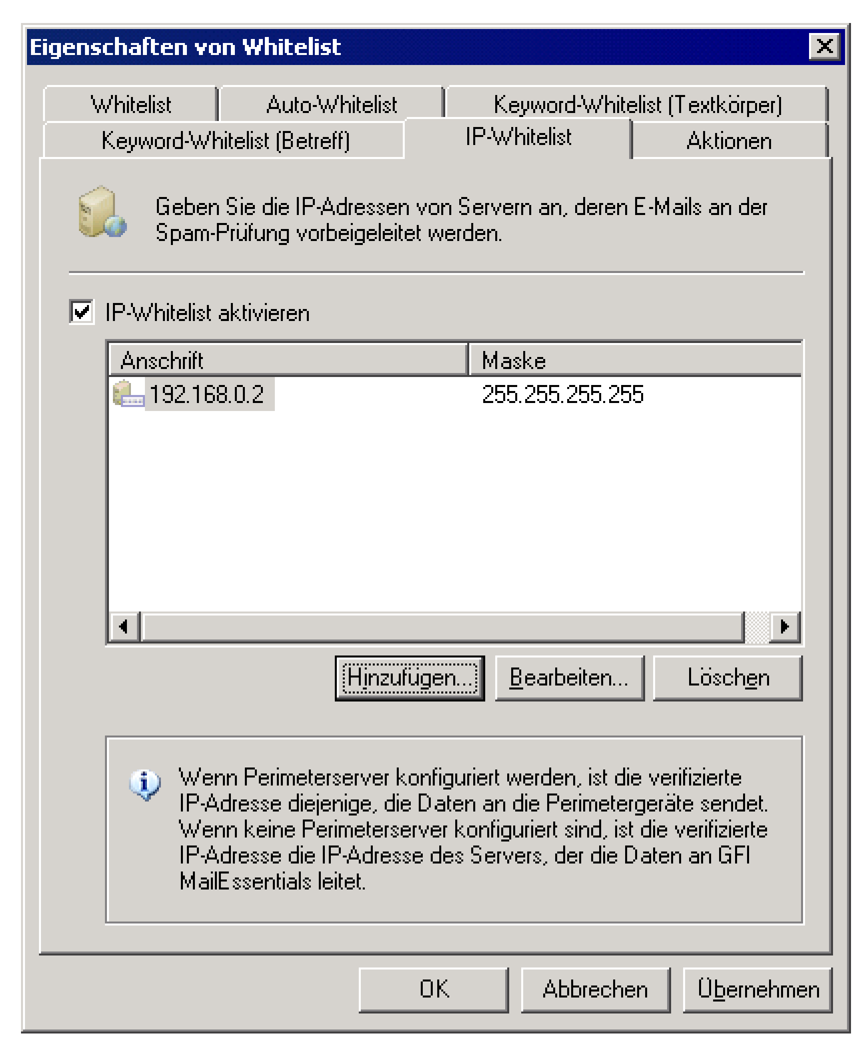


Bild 43 - Whitelist IPs

7. Legen Sie auf der Registerkarte **IP-Whitelist** die IP-Adressen fest, von denen zulässige E-Mails empfangen werden. Aktivieren Sie die Option **IP-Whitelist aktivieren**, um diese Funktion zu verwenden. Klicken Sie auf **Hinzu**, um eine einzelne IP-Adresse oder Subnetzmaske festzulegen, die die SPAM-Prüfung umgehen soll.

HINWEIS: Beim Hinzufügen von IP-Adressen zur IP-Whitelist können Sie auch einen Bereich von IP-Adressen in CIDR-Notation eingeben.

8. Klicken Sie auf die Registerkarte **Aktionen**, um die Protokollierung der Whitelist in einer Datei zu aktivieren oder zu deaktivieren. Klicken Sie auf **Durchsuchen**, um einen Ordner anzugeben, in dem die Protokolle gespeichert werden sollen.

9. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

Neue Absender

Der Filter "Neue Absender" erlaubt es GFI MailEssentials automatisch E-Mails von Absendern zu identifizieren, an die noch nie E-Mails gesendet wurden. Solche Absender werden durch einen Vergleich mit den in der Whitelist erfassten Daten identifiziert.

Nur E-Mails, in denen keine Spam-Nachrichten erkannt wurden, und deren Absender nicht in der Whitelist eingetragen sind, werden in den Ordner Neue Absender übertragen.

Da solche E-Mails auch von berechtigten Benutzern stammen können, werden sie in einem speziellen Ordner gesammelt. Auf diese Weise können die E-Mails einfach identifiziert werden. Danach können Sie diese E-Mails prüfen und nicht erkannte Spam-Nachrichten in die benutzerdefinierten Blockliste eintragen.

Dieser Filter ist standardmäßig NICHT aktiviert.

Wichtige Hinweise

1. Aktivieren Sie mindestens eine der verfügbaren Whitelists um die Funktion Neue Absender zu

verwenden. Wenn keine Whitelist zur Verfügung steht (wenn keine Spam durch andere Filter erkannt wurde), werden die empfangenen Nachrichten in das Empfängerpostfach übertragen. **Nur** E-Mails, in denen keine Spam-Nachrichten erkannt wurden, und deren Absender nicht in der Whitelist eingetragen sind, werden in den Ordner Neue Absender übertragen.

Konfiguration des Filters "Neue Absender"

1. Klicken Sie auf **Anti-Spam** ► **Neue Absender** ► **Eigenschaften**.

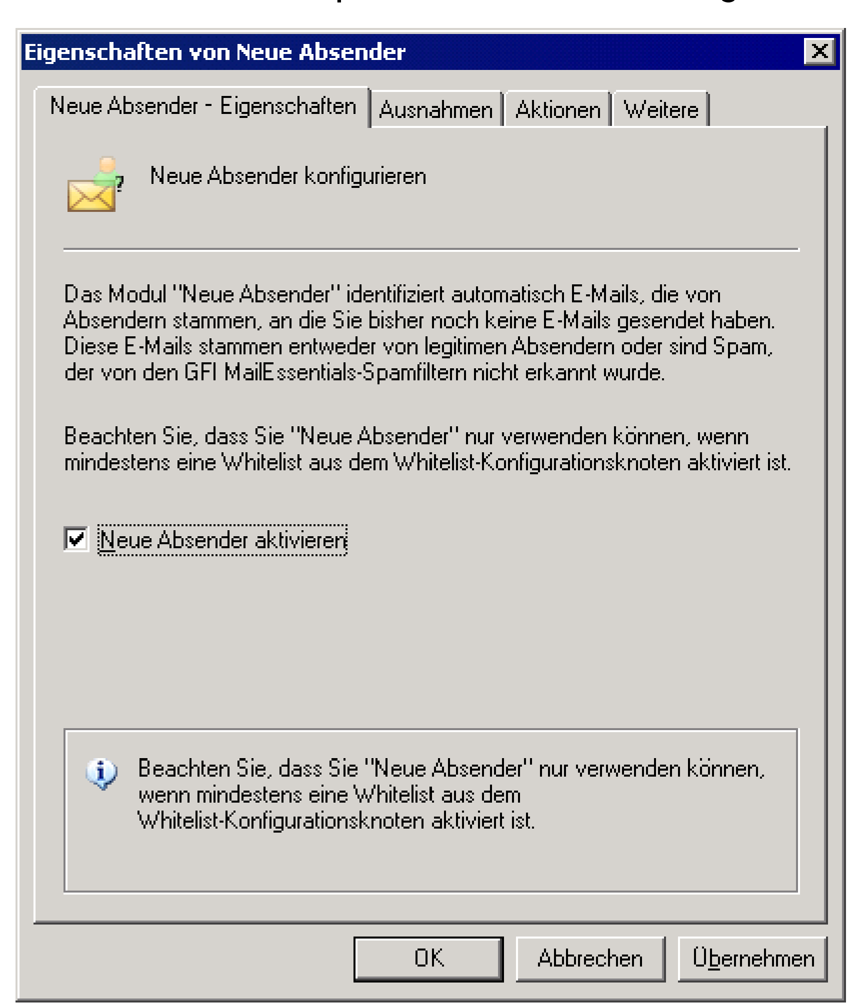


Bild 44 - Neue Absender - Eigenschaften

2. Klicken Sie auf der Registerkarte **Neue Absender - Eigenschaften** in das Kontrollkästchen **Neue Absender aktivieren** um die Prüfung aller eingehenden Nachrichten auf neue Absender zu aktivieren und klicken Sie auf **Übernehmen**.

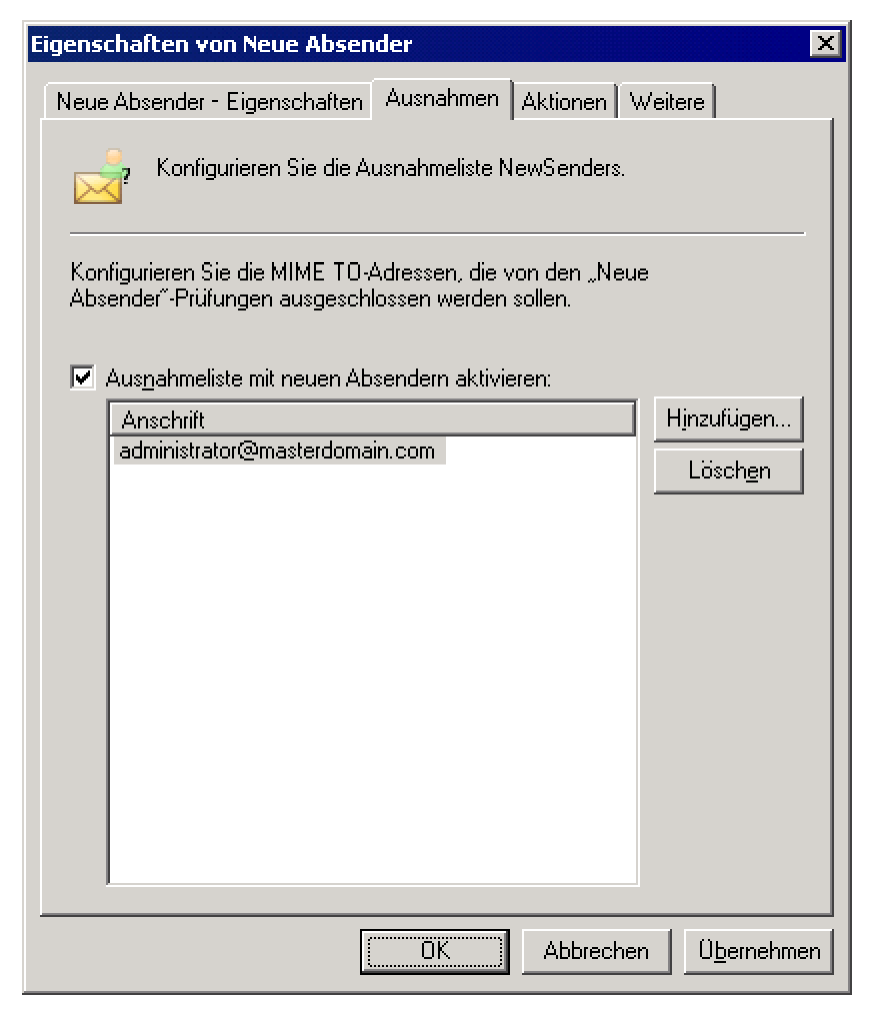


Bild 45 - Neue Absender-Ausnahmenkonfiguration

3. Klicken Sie auf die Registerkarte **Ausnahmen** und aktivieren Sie das Kontrollkästchen **MIME TO Ausnahmeliste:** um die lokalen Empfänger zu konfigurieren, deren E-Mails bei der Prüfung auf neue Absender ausgeschlossen werden sollen.

4. Klicken Sie auf die Schaltfläche **Hinzufügen** … und geben Sie die E-Mail-Adresse des Absenders ein.

- Beispiel: **administrator@master-domain.com**.

Wiederholen Sie dies für jede Adresse, die Sie hinzufügen wollen, und klicken Sie zum Speichern auf die Schaltfläche **Übernehmen**.

HINWEIS: Um Ihre Ausnahmeliste vorübergehend zu deaktivieren, müssen Sie nicht alle eingetragenen Adressen löschen, sondern brauchen nur das Kontrollkästchen **MIME TO Ausnahmeliste:** zu deaktivieren.

5. Klicken Sie auf die Registerkarte **Aktionen** um die Aktionen auszuwählen, die bei als Spam identifizierten Nachrichten durchgeführt werden sollen. Weitere Informationen über Spam-Aktionen finden Sie in dem Abschnitt Spam-Aktionen - Umgang mit Spam-Mails in diesem Handbuch.

6. Klicken Sie auf **OK** um die Konfiguration abzuschließen.

Sortieren von Spam-Filtern nach Priorität

In GFI MailEssentials können Sie die Reihenfolge festlegen, in der Spam-Prüfungen für eingehende Nachrichten ausgeführt werden.

HINWEIS: Die Reihenfolge aller verfügbaren Filter können Sie anpassen. Nur der Neue Absender hat automatisch immer die niedrigste Priorität. Dies hängt damit zusammen, dass zuvor die Ergebnisse der Whitelist sowie der anderen Spam-Filter geprüft werden müssen.

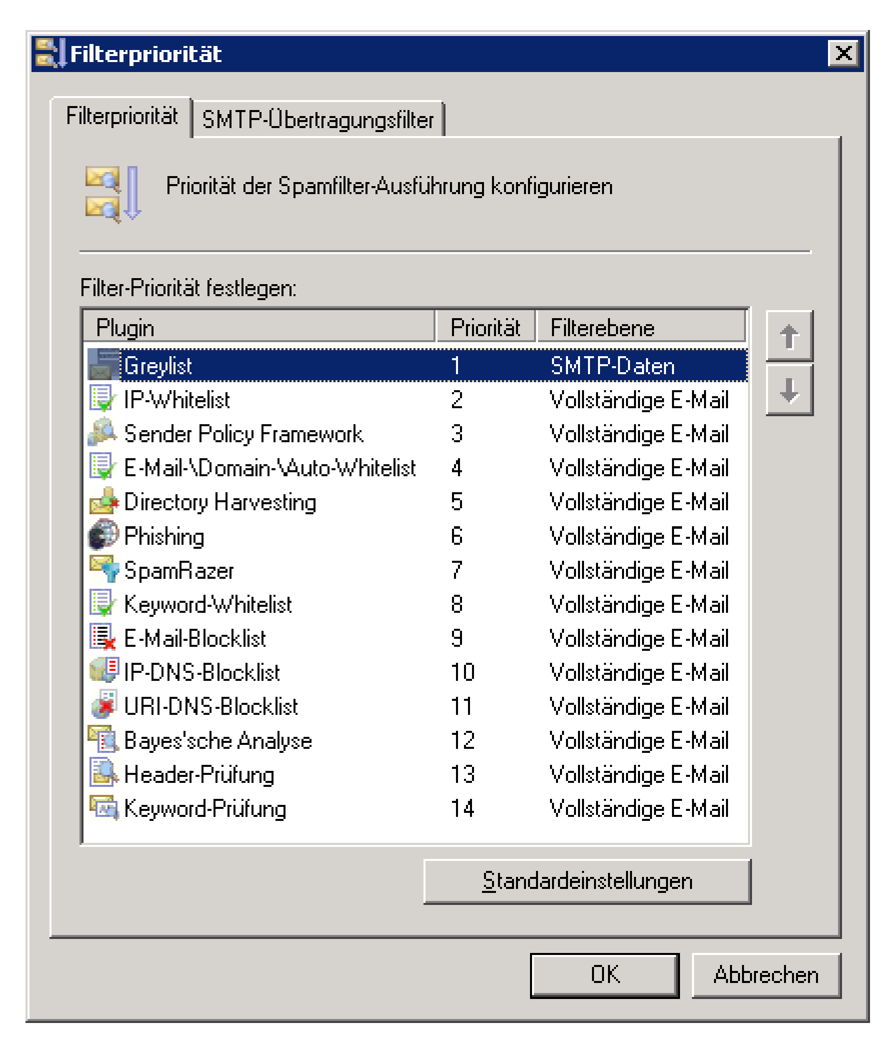


Bild 46 - Zuordnung von Filterprioritäten

1. Klicken Sie mit der rechten Maustaste auf den Knoten **Anti-Spam** ► **Filterpriorität** und dann auf **Eigenschaften**.

2. Klicken Sie auf einen Filter und dann auf die Schaltfläche <Aufwärts> um den ausgewählten Filter eine höhere Priorität zuzuordnen oder auf die Schaltfläche <Abwärts> um dem ausgewählten Filter eine niedrigere Priorität zu geben.

HINWEIS: Klicken Sie auf die Schaltfläche **Standardeinstellungen** um die Filterreihenfolge wieder auf den Standard einzustellen.

3. Klicken Sie auf die Schaltfläche **OK** um die Konfiguration zu übernehmen. Die Änderungen werden sofort wirksam.

5.2 Spam-Aktionen - Umgang mit Spam-Mails

Die Registerkarten **Aktionen** und **Weitere** in den Spam-Filterdialogen legen fest, wie mit Spam-Mails verfahren werden soll. Für jeden einzelnen Spam-Filter können Sie andere Aktionen definieren.

- **Beispiel:** Löschen Sie E-Mails, die durch den SpamRazer gekennzeichnet wurden, nicht aber E-Mails, die durch die Keyword-Prüfung als Spam markiert wurden.

Konfiguration von Spam-Aktionen

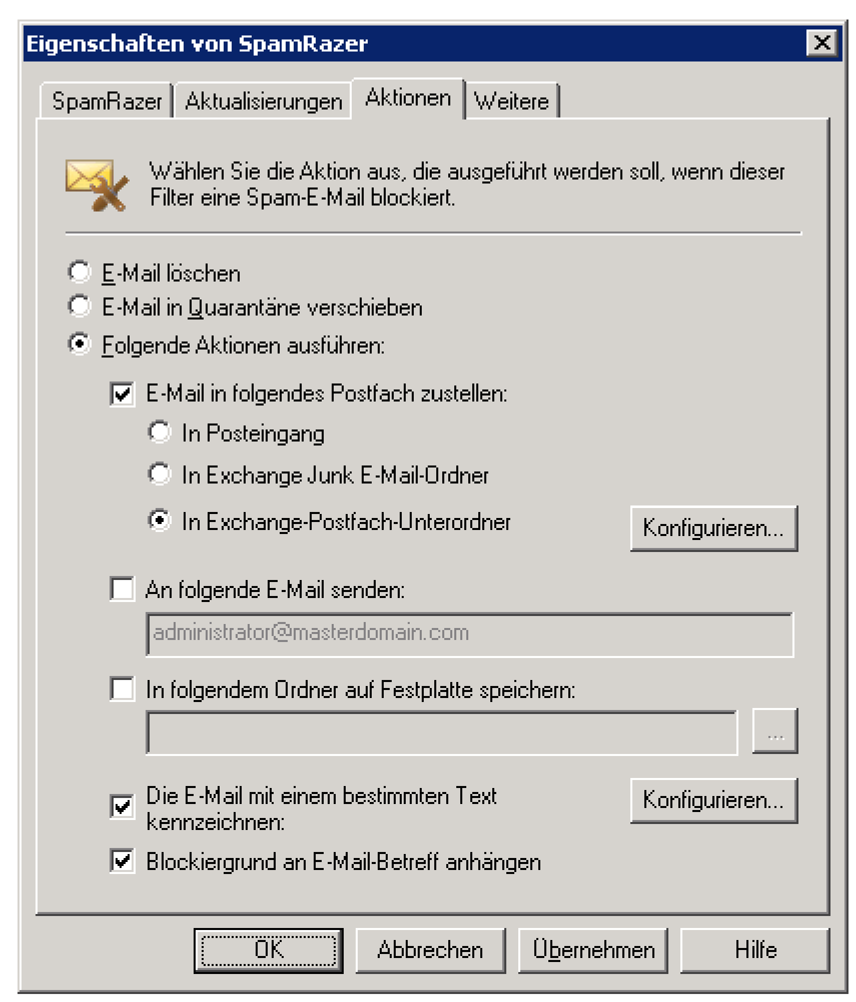


Bild 47 - Konfiguration der gewünschten Aktion

1. Klicken Sie auf der Registerkarte **Aktionen** auf eine Option, die festlegt, welche Aktion bei als Spam markierten E-Mails durchgeführt werden soll:

- **E-Mail löschen** - Löscht eine E-Mail, die durch einen bestimmten Spamfilter geblockt ist. Andere Spamoptionen werden deaktiviert, sobald die E-Mail gelöscht ist.
- **E-Mail in Quarantäne verschieben** - Als Spam erkannte E-Mails werden im Quarantänespeicher abgespeichert. Andere Spam-Aktionen sind deaktiviert, wenn die E-Mail in Quarantäne verschoben wird. Weitere Informationen finden Sie im Abschnitt **Verwenden der Quarantäne**.
- **E-Mail in Postfach verschieben** - Wählen Sie den Ordner aus, in dem die E-Mail gespeichert werden soll:
  - **Im Posteingang** - Mit dieser Option leiten Sie die Spam-Mails in den Posteingang des Benutzers.
  - **In Exchange-Junk-Ordner des Benutzers verschieben** - Mit dieser Option verschieben Sie alle Spam-Mails in den Standard-Junk-Ordner des Benutzers.

- **In den Postfach-Unterordner von Microsoft Exchange -** Mit dieser Option leiten Sie alle Spams in einen bestimmten Ordner des Benutzerpostfachs um. Klicken Sie auf **Konfigurieren**, um den Dialog "In Exchange-Ordner verschieben" zu starten und geben Sie den Ordner ein, in den die Spam-E-Mails verschoben werden sollen.
  - **Beispiel 1:** Geben Sie **vermutliche Spam** für einen benutzerdefinierten Ordner ein, der auf der gleichen Ebene wie der Posteingangsordner erstellt werden soll.
  - **Beispiel 2:** Geben Sie **Posteingang\vermutliche Spam** für einen benutzerdefinierten Ordner ein, der im Eingangspostfach erstellt werden soll.

  HINWEIS 1: Für diese Option müssen folgende Bedingungen erfüllt sein:

  - GFI MailEssentials muss auf einem Computer mit Microsoft Exchange Server installiert sein. Ist GFI MailEssentials nicht auf einem Microsoft Exchange Server installiert, verfahren Sie entsprechend dem Kapitel **Verschieben von Spam-E-Mails in den Postfachordner des Benutzers** in diesem Handbuch
  - Die Active Directory muss aktiviert sein.
  - Es muss Microsoft Exchange Server 2003 bzw. Microsoft Exchange Server 2007/2010 mit der Mailbox-Serverrolle vorhanden sein.

  HINWEIS 2: Damit diese Option aktiviert werden kann, ist bei Microsoft Exchange 2010 ein dezidierter Benutzer erforderlich. Klicken Sie im Dialog Aktionen auf **Konfigurieren** und dann auf **Benutzerkonto festlegen**, um den dezidierten Benutzer zu definieren. Wählen Sie im Konfigurationsdialog In Exchange verschieben eine der folgenden Optionen aus:

  - **Spam mit automatisch erstelltem Benutzer verschieben -** Wählen Sie diese Option aus, damit GFI MailEssentials automatisch einen Benutzer mit allen erforderlichen Rechten einrichten kann.
  - **Spam in folgendes Benutzerkonto verschieben -** Wählen Sie diese Option aus, um einen manuell erstellten Benutzer zu verwenden. Geben Sie die Anmeldedaten (Domäne\Benutzername und Kennwort) eines dezidierten Benutzers an und klicken Sie auf **Zugriffsrechte definieren**, um dem angegebenen Benutzer die erforderlichen Rechte zuzuweisen.

  HINWEIS: Die manuell angegebenen Benutzeranmeldedaten dürfen nur für diese Funktion gelten. Benutzername, Kennwort und sonstige Eigenschaften dürfen NICHT von Microsoft Exchange oder Active Directory abweichen, sonst funktioniert die Funktion zum Verschieben in den Exchange-Ordner nicht.

» **An E-Mail-Adresse weiterleiten -** Die als Spam gekennzeichnete E-Mail wird an eine spezifische E-Mail-Adresse weitergeleitet.

- **Beispiel:** Eine E-Mail-Adresse eines öffentlichen Ordners. Auf diese Weise kann jemand beauftragt werden, regelmäßig die als Spam gekennzeichneten E-Mails zu überprüfen und E-Mails zu identifizieren, die fälschlicherweise als Spam gekennzeichnet wurden.

Der Betreff der E-Mail hat das Format **[recipient] [subject]**

» **In definierten Ordner auf Festplatte speichern -** Speichert alle als Spam markierten E-Mails unter dem angegebenen Pfad.

- **Beispiel:** 'C:\Spam\'.

Der Dateiname der gespeicherten E-Mail hat folgendes Format:

`[Sender_recipient_subject_number_.eml]` (Beispiel: `C:\Spam\jim@comp.com_bob@comp.com_MailOffers_1_.eml`)

» **E-Mail mit bestimmtem Text markieren -** Mit dieser Option ergänzen Sie einen Text in der E-Mail-Betreffzeile. Klicken Sie auf **Konfigurieren**, um die Kennzeichnungsoptionen zu ändern. Geben Sie in dem Dialog "E-Mail kennzeichnen" den Text ein, den Sie für die Kennzeichnung verwenden wollen und geben Sie an, wo die Kennzeichnung platziert werden soll:

- **Vor Betreff einfügen** - Die angegebene Kennzeichnung wird am Anfang eingefügt, das heißt als Präfix, vor dem Betreff der E-Mail.
  - **Beispiel:** '[SPAM] Kostenlose Web-Mail-Adresse'.
- **An Betreff anhängen** - Die definierte Kennzeichnung wird am Ende, das heißt als Suffix, am Text der Betreffzeile angehängt.
  - **Beispiel:** 'Kostenlose Web-Mail-Adresse (Spam])'.
- **Kennzeichnung in neuem X-Header hinzufügen...** - Die definierte Kennzeichnung wird als neuer X-Header in der E-Mail eingefügt. In diesem Fall hat der X-Header folgendes Format:

  `X-GFIME-SPAM: [TAG TEXT]`

  `X-GFIME-SPAM-REASON: [GRUND]`

  - Beispiel:

  `X-GFIME-SPAM: [Das ist SPAM]`

  `X-GFIME-SPAM-REASON: [IP-DNS-Blocklist Prüfung fehlgeschlagen - Versand über Blockliste-Domäne]`

» **Grund für die Blockierung an E-Mail-Betreff anhängen -** Wenn Sie diese Option auswählen, werden der Name des Filters, der die E-Mail blockiert hat und der Grund für die Blockierung in der Betreffzeile der blockierten E-Mail angehängt.

Weitere Optionen

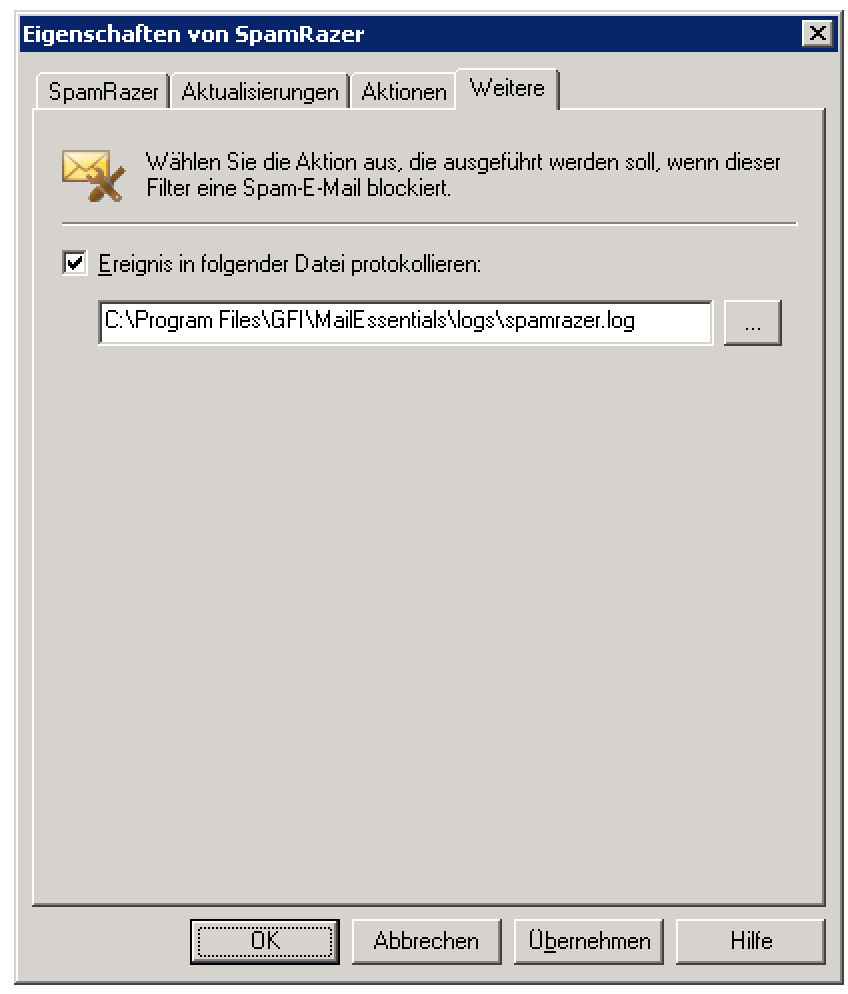


Bild 48 - Registerkarte "Weitere Aktionen"

Klicken Sie auf die Registerkarte **Weitere** um eine Reihe von Zusatzaktionen zu definieren:

» **Häufigkeit in dieser Datei protokollieren** - Protokollieren Sie die Häufigkeit der Spam-Mail in einer von Ihnen definierten Protokolldatei.

HINWEIS: Protokolldateien können sehr groß werden. GFI MailEssentials verfügt über einen Protokollrotator, durch den regelmäßig neue Protokolldateien erstellt werden, sobald eine Protokolldatei eine bestimmte Größe erreicht. Um den Protokollrotator zu aktivieren, öffnen Sie **Anti-Spam ► Anti-Spam-Einstellungen**. Aktivieren Sie auf der Registerkarte **Anti-Spam-Protokolle** die Option **Protokollrotator aktivieren**. Legen Sie die Rotationsbedingung nach Zeit oder Dateigröße fest.

HINWEIS: Falls die Installation von GFI MailEssentials ein Upgrade der Version 14 oder älter ist, bei der die Aktion des gefälschten Unzustellbarkeitsberichts (NDR) verwendet wurde, wurde diese übernommen. Diese Funktion ist nicht in GFI MailEssentials 2010 enthalten, da es eine Bedrohung für das Mail-Fluss-System ist. Weitere Informationen zum Senden von gefälschten NDRs finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID002898

Globale Spam-Aktionen

Viel Spam wird an E-Mail-Adressen versendet, die nicht mehr existieren. Allgemein werden diese E-Mails einfach gelöscht, zur Problembehandlung oder für Testzwecke können Sie diese E-Mails jedoch in einen Ordner verschieben oder an eine bestimmte E-Mail-Adresse weiterleiten.

HINWEIS: Dieser Abschnitt bezieht sich nur auf Installationen von Microsoft Exchange Server, bei denen die Funktion **In Spam-Ordner des Benutzers weiterleiten** aktiviert ist. Bei anderen Servern wird die Registerkarte "Globale Spam-Aktionen" nicht angezeigt.

Konfiguration der globalen Spam-Aktionen

1. Klicken Sie mit der rechten Maustaste auf den Knoten **Anti-Spam ► Anti-Spam-Einstellungen** und dann auf **Eigenschaften**.

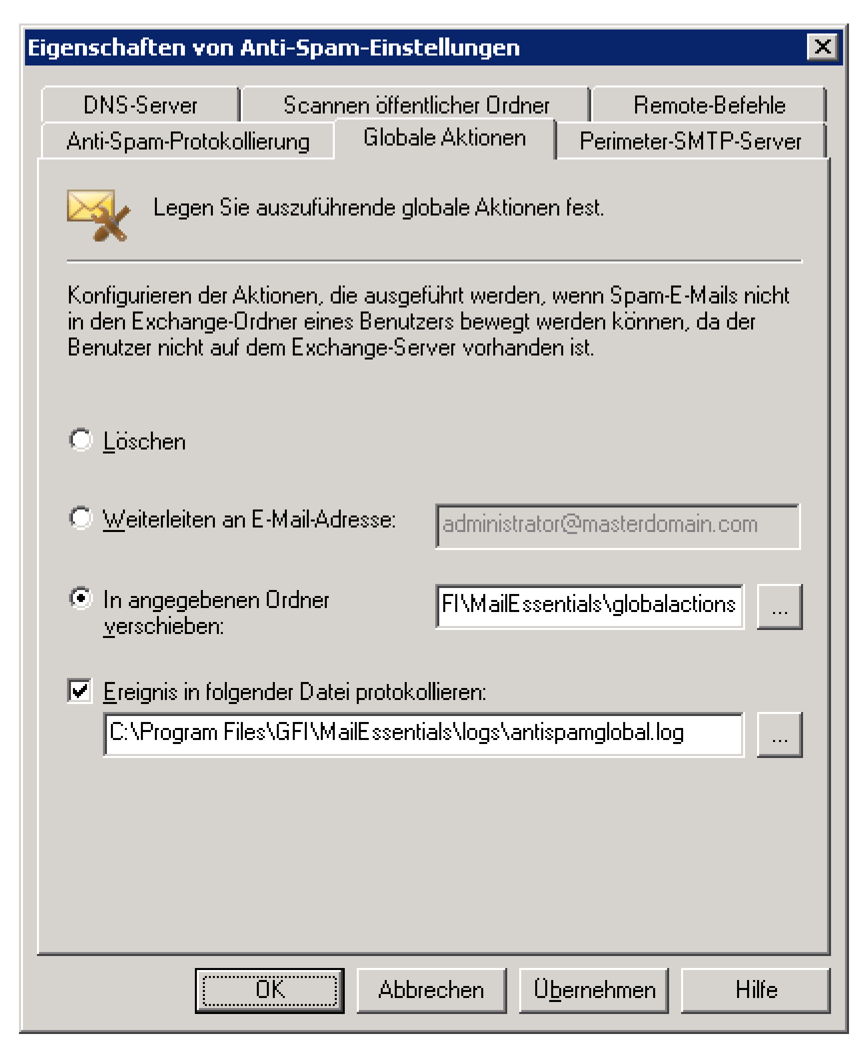


Bild 49 - Globale Aktionen

2. Klicken Sie auf die Registerkarte **Globale Aktionen** und wählen Sie eine der folgenden Optionen aus:

- E-Mail löschen
- E-Mail an eine bestimmte E-Mail-Adresse weiterleiten
- E-Mail in einen definierten Ordner verschieben

3. Klicken Sie auf **Häufigkeit in dieser Datei protokollieren** um eine Spam-Mail in einer Protokolldatei zu erfassen.

5.3 Konfigurieren der Quarantäne

Die Quarantäne von GFI MailEssentials ist ein zentraler Speicher, wo alle als Spam erkannten, eingehenden E-Mails für einige Tage verbleiben. Dies stellt sicher, dass Benutzer keinen Spam empfangen, und die für die Verarbeitung dieser E-Mails verwendeten Ressourcen auf dem Mailserver werden reduziert.

Administratoren und E-Mail-Benutzer können die E-Mails in Quarantäne anzeigen, indem Sie mit einem Webbrowser auf die Quarantäneoberfläche zugreifen. GFI MailEssentials kann außerdem reguläre E-Mail-Berichte an E-Mail-Benutzer senden, um über die blockierten E-Mails zu informieren.

Wichtige Hinweise

1. Ändern Sie die Aktion eines Spam-Filters, mit dem Sie eine **E-Mail in Quarantäne verschieben** möchten. Weitere Informationen finden Sie unter **Spam-Aktionen - Umgang mit Spam-Mails**.

2. Der Quarantänespeicher von GFI MailEssentials benötigt Festplattenspeicher, um Spam-E-Mails des Unternehmens für einige Tage aufzubewahren. Der erforderliche Festplattenspeicher hängt von Folgendem ab:

- die Menge an erhaltenem Spam,
- die Dauer der Aufbewahrung im Quarantänespeicher.

Durchschnittlich benötigen 100.000 Spam-E-Mails mit einer Größe von jeweils 5 KB einschließlich der Metadaten etwa 600 MB Festplattenspeicher.

3. Falls der freie Festplattenspeicher am Speicherort des Quarantänespeichers gleich oder kleiner als 512 MB ist, stoppt GFI MailEssentials das Verschieben von Spam-E-Mails in die Quarantäne. Spam-E-Mails werden gekennzeichnet und dem Empfängerpostfach zugestellt, bis der freie Speicherplatz größer als 512 MB ist. Das stellt sicher, dass die Festplatte nicht voll wird.

4. Die Quarantänefunktion von GFI MailEssentials erfordert den Microsoft ISS WWW-Dienst.

5.3.1 Konfigurieren der Quarantäne

1. Starten Sie die Konfigurationskonsole von GFI MailEssentials, indem Sie auf **Start** ► **Programme** ► **GFI MailEssentials** ► **GFI MailEssentials-Konfiguration** klicken.

2. Klicken Sie mit der rechten Maustaste auf **Anti-Spam** ► **Quarantäne** ► **Quarantäneeinstellungen** und anschließend **Eigenschaften**.

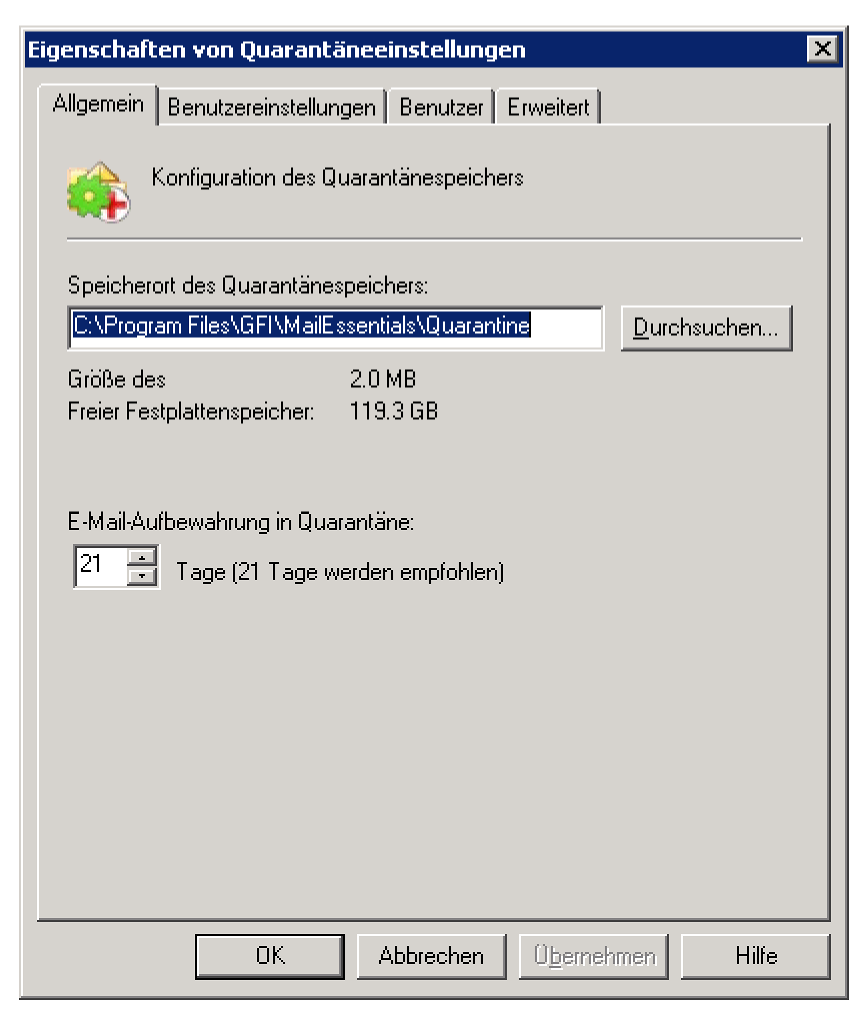


Bild 50 - Quarantäneeinstellungen

3. Legen Sie auf der Registerkarte **Allgemein** Folgendes fest:

» **Speicherort des Quarantänespeichers** - Klicken Sie auf **Durchsuchen**, um den Pfad festzulegen, unter dem der Quarantänespeicher gespeichert werden soll. Der Standardpfad ist *<Installationsordner von GFI MailEssentials>\Quarantine*.

WICHTIG: Stellen Sie sicher, dass die Partition, auf der der Quarantänespeicher gespeichert werden soll, über ausreichend freien Speicherplatz verfügt. Spam-E-Mails werden nicht in die Quarantäne verschoben, wenn der Festplattenspeicher gleich oder kleiner als 512 MB ist. Beim Erreichen von 512 MB stellt die E-Mail-Quarantäne den Betrieb ein, Spam wird als solcher gekennzeichnet und dem Empfängerpostfach zugestellt, bis der freie Speicherplatz größer als 512 MB ist.

» **E-Mail-Aufbewahrung in Quarantäne** - Legen Sie die Anzahl der Tage fest, die die E-Mails im Quarantänespeicher verbleiben.

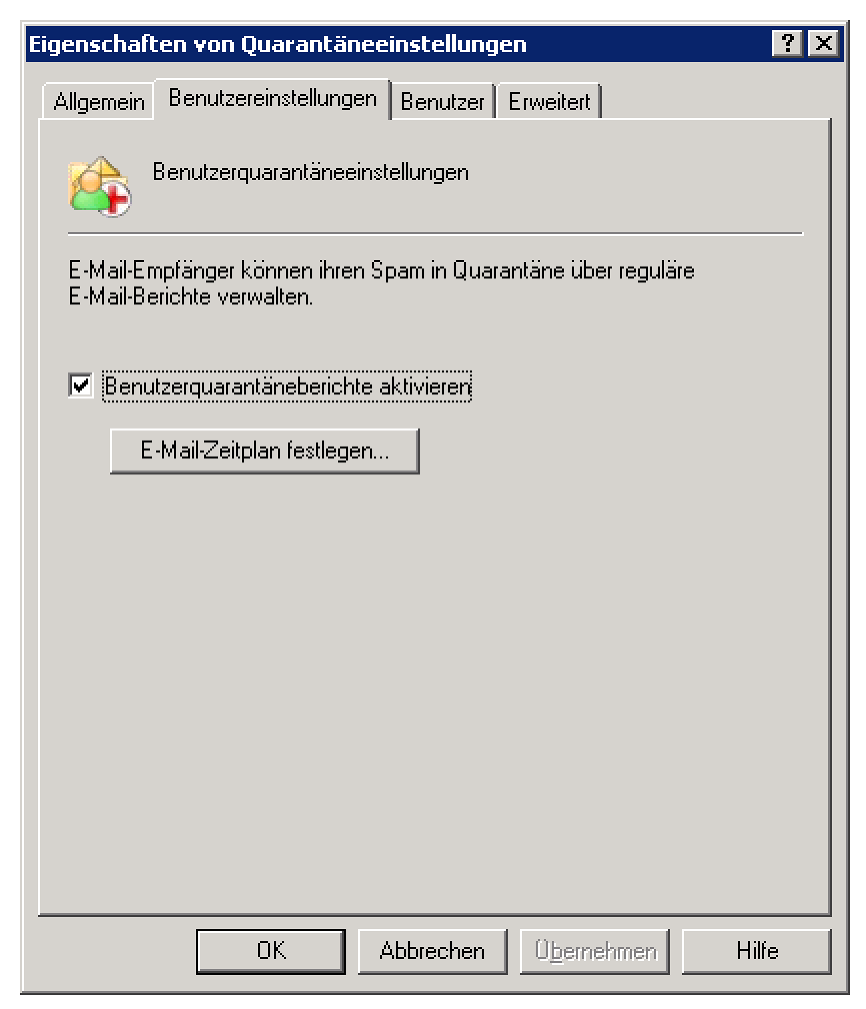


Bild 51 - Benutzereinstellungen

4. Benutzerquarantäneberichte sind regelmäßige E-Mails an die E-Mail-Benutzer, die eine Liste der blockierten E-Mails enthalten. Benutzer können die Liste anzeigen, um zulässige E-Mails, die blockiert wurden, zuzulassen. Um die E-Mail-Berichte zu aktiveren, aktivieren Sie auf der Registerkarte **Benutzereinstellungen** die Option **Benutzerquarantäneberichte aktivieren**.

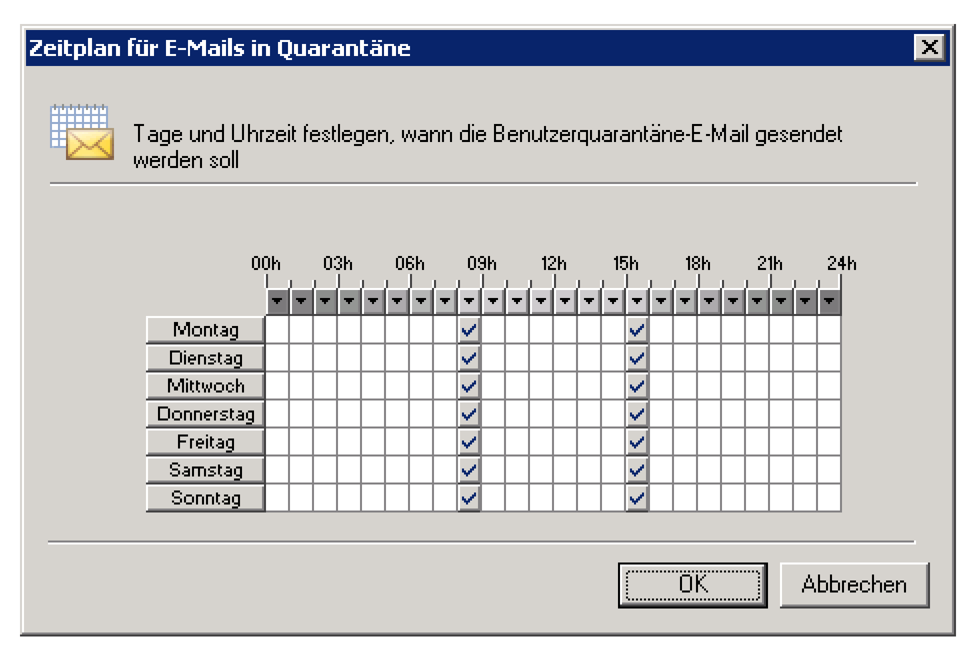


Bild 52 - Quarantäne-E-Mail-Zeitplan

5. Klicken Sie auf **E-Mail-Zeitplan festlegen...**, um die Wochentage und Uhrzeit festzulegen, an denen der Quarantäne-E-Mail-Bericht gesendet werden soll. Klicken Sie auf **OK**, um den Zeitplan zu übernehmen.

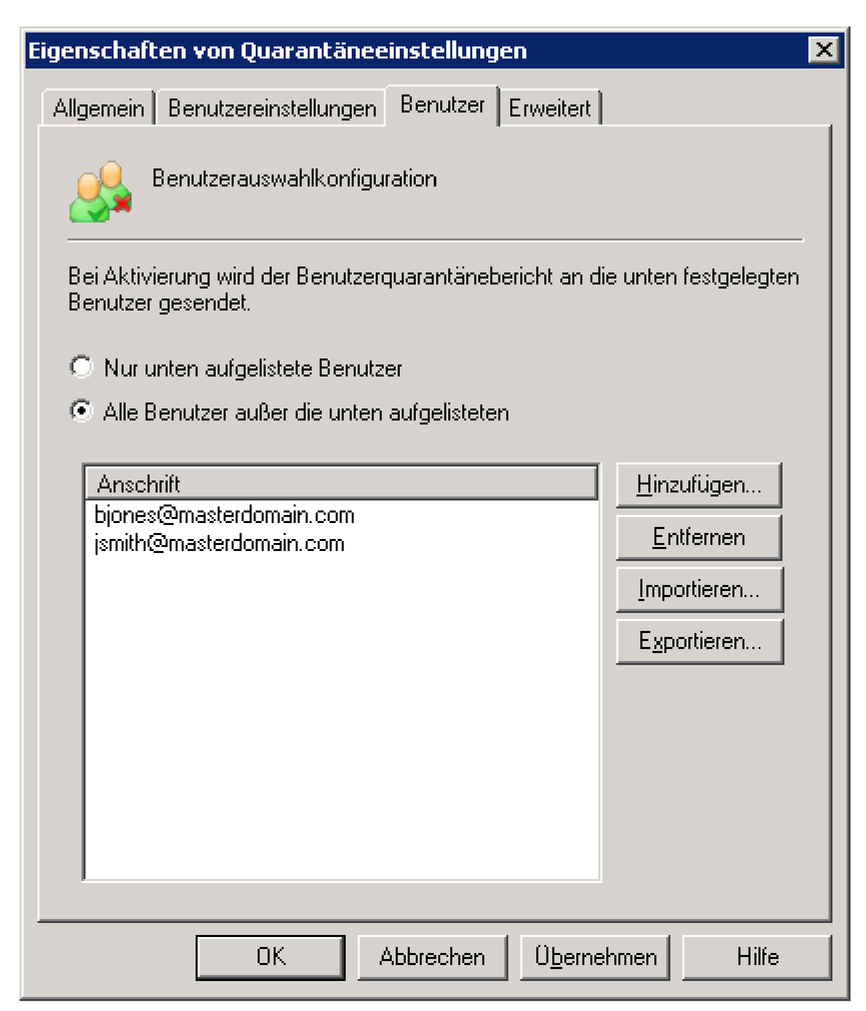


Bild 53 - Auswahl der Benutzer, die einen Quarantäne-E-Mail-Bericht empfangen sollen

6. Wechseln Sie bei Aktivierung der Quarantäne-E-Mail-Berichte auf die Registerkarte **Benutzer**, und legen Sie die Empfänger fest, die einen Bericht empfangen sollen. Wählen Sie:

» **Nur unten aufgelistete Benutzer** - Nur die in der Liste aufgeführten Benutzer erhalten einen Quarantäne-E-Mail-Bericht.

- **Alle Benutzer außer die unten aufgelisteten** - Alle E-Mail-Benutzer außer die in der Liste aufgeführten erhalten einen Quarantäne-E-Mail-Bericht.

7. Legen Sie abhängig von der Auswahl in Schritt 7 die E-Mail-Adressen fest, die der Liste hinzugefügt werden sollen. Klicken Sie auf:

- **Hinzu**, um hinzuzufügende E-Mail-Adressen manuell hinzuzufügen.
- **Entfernen**, um die Benutzer auszuwählen, die von der Liste entfernt werden sollen. Klicken Sie auf **Entfernen**.
- **Importieren**, um eine Liste von E-Mail-Adressen aus einer xml-Datei zu importieren.
- **Exportieren**, um eine Liste von E-Mail-Adressen in eine xml-Datei zu exportieren.

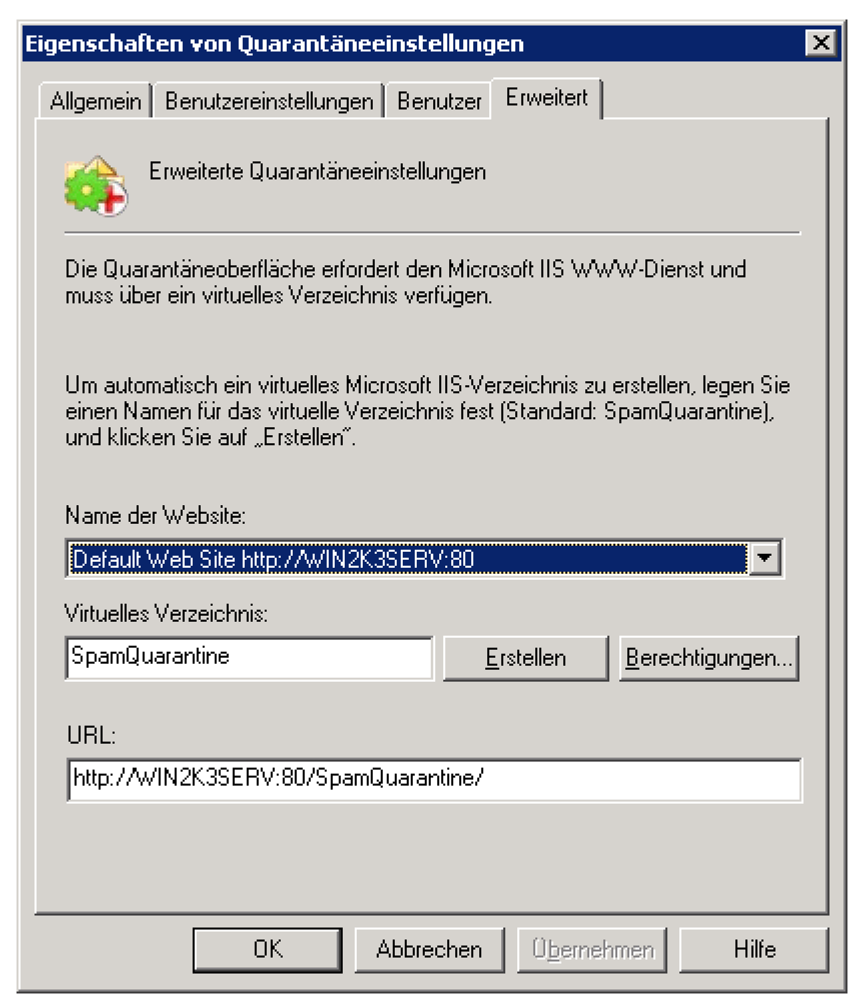


Bild 54 - Konfigurieren von erweiterten Quarantäneeinstellungen

8. Legen Sie auf der Registerkarte **Erweitert** erweiterte Einstellungen fest. Konfigurieren Sie:

- **Name der Website** - Wählen Sie die Website aus, über die auf die Quarantäneoberfläche im Webbrowser zugegriffen werden kann.
- **Virtuelles Verzeichnis** - Geben Sie einen Namen für das virtuelle Verzeichnis ein, und klicken Sie auf **Erstellen**, um automatisch ein virtuelles Verzeichnis zu erstellen. Der Standardname ist „SpamQuarantine".
- **Berechtigungen…** - Startet ein separates Dialogfeld, um die Benutzer oder Gruppen anzugeben, die uneingeschränkten Zugriff auf alle E-Mails in Quarantäne haben.
- **URL** - (Optional) Die Standard-URL, die in Benutzerquarantäneberichten für den Zugriff auf die Quarantäneoberfläche verwendet wird. Diese wird im folgenden Format angegeben:

```
http://<Name des Webservers>/<Virtuelles Verzeichnis>
```

Auf diese URL kann jedoch nicht über das Internet zugegriffen werden. Wenn eine öffentliche Domäne verfügbar ist, können Sie den Namen des Webservers manuell in eine öffentliche Domäne ändern, auf die über das Internet zugegriffen werden kann. Diese URL wird nun von Links in Quarantäne-E-Mail-Berichten für Benutzer verwendet.

Weitere Informationen nur Nutzung der Quarantäne finden Sie unter Verwenden der Quarantäne.

5.4 Scannen öffentlicher Ordner

Die Spammer entwickeln ihre Verfahren laufend weiter, daher kommt es immer wieder vor, dass Spam-Mails von Spam-Filtern nicht erkannt werden und ins Postfach des Empfängers gelangen. Durch das Scannen öffentlicher Ordner können die Benutzer manuell E-Mails als Spam kennzeichnen und die Spam-Filter von GFI MailEssentials trainieren, damit ähnliche E-Mails als Spam erkannt werden.

Beim Scannen öffentlicher Ordner lädt GFI MailEssentials E-Mails aus den öffentlichen Ordnern und ergänzt diese in der Whiteliste/Blockliste sowie in der HAM/SPAM-Datenbank. Bei Systemen mit Microsoft Exchange Server oder Lotus Domino werden öffentliche Ordner automatisch nach Abschluss der Konfiguration erstellt.

Führen Sie die in den folgenden Abschnitten aufgeführten Anweisungen aus um das Scannen öffentlicher Ordner zu aktivieren.

5.4.1 Konfiguration des Scannens öffentlicher Ordner für Microsoft Exchange Server

1. Klicken Sie in der Konfigurationskonsole für GFI MailEssentials mit der rechten Maustaste auf den Knoten **Anti-Spam ► Anti-Spam Einstellungen** und wählen Sie die Option **Eigenschaften**.

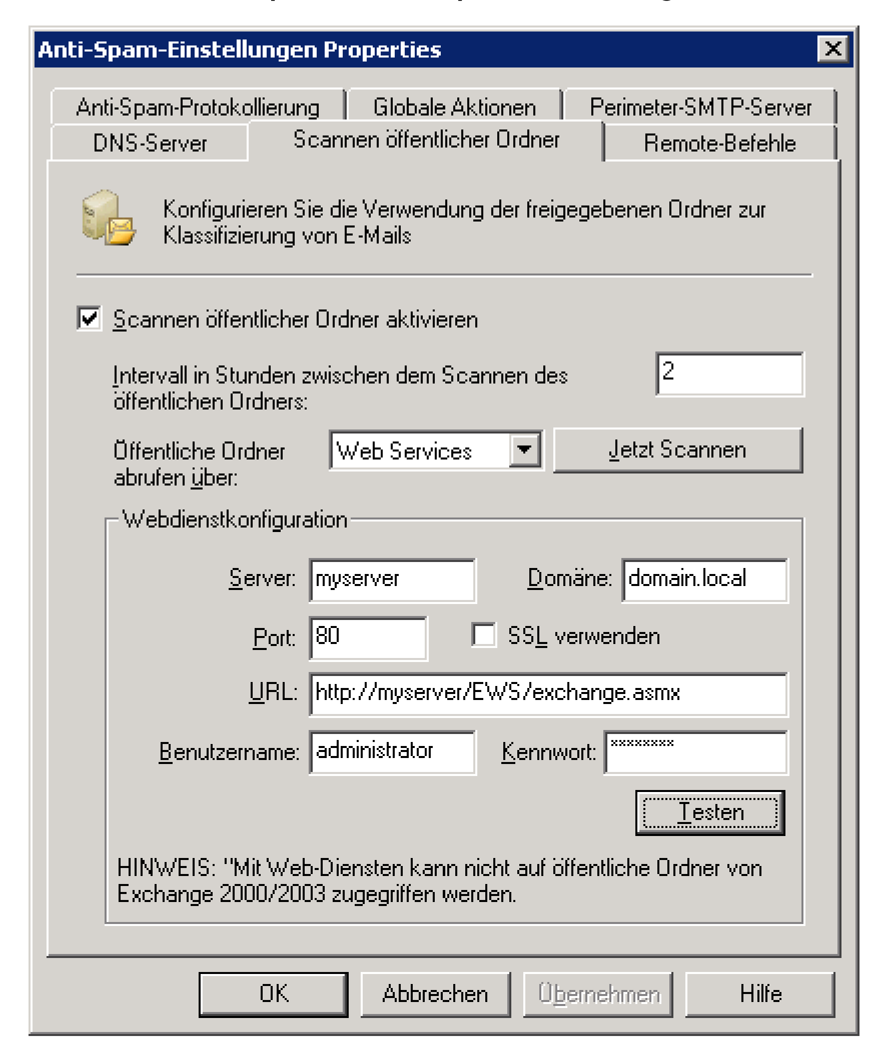


Bild 55 - Konfigurtion des Scannens öffentlicher Ordner

2. Klicken Sie auf die Registerkarte **Scannen öffentlicher Ordner** und dann in das Kontrollkästchen **Scannen öffentlicher Ordner** aktivieren.

3. Wählen Sie aus der Anzeigeliste **Öffentliche Ordner abrufen über** das Verfahren aus, mit dem GFI MailEssentials die E-Mails aus öffentlichen Ordnern holen soll.

- **Für Exchange Server 2003 -** Wählen Sie MAPI, IMAP oder WebDAV.
- **Für Exchange Server 2007 -** Wählen Sie WebDAV oder Web Services.
- Für Exchange Server 2010 - Wählen Sie Web Services.

Verfügbare Optionen:

- **MAPI** - Damit MAPI verwendet werden kann, muss GFI MailEssentials auf dem Computer installiert sein, auf dem auch Microsoft Exchange Server installiert ist. Weitere Einstellungen sind nicht erforderlich.
- **IMAP** - Erfordert Microsoft Exchanges IMAP-Service. IMAP erlaubt ein Scannen öffentlicher Ordner aus der Ferne und arbeitet bei Umgebungen mit Firewalls ausgezeichnet. Außerdem kann IMAP auch bei anderen Mailservern eingesetzt werden, die IMAP unterstützen. Benötigte Parameter:
  - Mail-Servername
  - Portnummer (Standard-IMAP-Port ist 143)
  - Benutzername/Kennwort
  - Wählen Sie für eine sichere Verbindung die Option **SSL verwenden**.
- **WebDAV** - Geben Sie den Namen des Mailservers, den Port (Standardport für WebDAV ist 80), den Benutzernamen, das Kennwort und die Domäne ein. Markieren Sie für eine sichere Verbindung das Kontrollkästchen **SSL verwenden**. Standardmäßig sind öffentliche Ordner in dem virtuellen Verzeichnis 'public' erreichbar. Wenn diese Einstellung verändert wurde, geben Sie den korrekten Namen des virtuellen Verzeichnisses ein um auf die öffentlichen Ordner zuzugreifen; bearbeiten Sie dazu den Text in dem Feld URL.
- **Web-Dienste** - Geben Sie folgende Informationen an:
  - **Server** - Name des Mailservers
  - **Domäne** - Lokale Domäne

    HINWEIS: Wenn sowohl eine lokale als auch eine öffentliche Domäne vorhanden sind, verwenden Sie die lokale Domäne.
  - **Port** - Standardport für Web-Dienste (80, bei SSL 443).
  - **Benutzername/Kennwort** - Verwenden Sie Anmeldeinformationen mit administrativen Berechtigungen, oder erstellen Sie ein dediziertes Benutzerkonto mit Microsoft Exchange Management Shell, indem Sie folgenden Befehl eingeben, um die erforderlichen Berechtigungen hinzuzufügen:

    ```
    Add-ADPermission -identity "Postfachspeicher" -User NewUser -
    AccessRights GenericALL
    ```

    HINWEIS: Ersetzen Sie „`Postfachspeicher`“ mit dem Namen des Postfachspeichers, der die Benutzerpostfächer enthält, und ersetzen Sie „`NewUser`“ mit dem Benutzernamen des erstellten Benutzers.
  - **SSL verwenden** - Wählen Sie diese Option aus, wenn für Exchange Web Services eine sichere Verbindung erforderlich ist. Web Services erfordern standardmäßig SSL.
  - **URL** - Öffentliche Ordner sind standardmäßig im virtuellen Verzeichnis „EWS/exchange.asmx“ verfügbar. Bearbeiten Sie den Text im Feld **URL**, wenn diese Einstellung geändert wurde, um den Namen des richtigen virtuellen Verzeichnisses für den Zugriff auf die öffentlichen Ordner anzugeben.

HINWEIS: Es wird empfohlen, die Einstellungen durch Laden der URL in einem Webbrowser manuell zu überprüfen. Bei diesem Vorgang sollte die formatierte XML-Datei **services.wsdl** geladen werden.

4. Klicken Sie auf **Jetzt scannen** um automatisch öffentliche Ordner zu erstellen.

5. Klicken Sie auf **Testen**, wenn Sie IMAP WebDAV oder Web Services konfigurieren. Sie erhalten auf dem Bildschirm einen Hinweis über Erfolg oder Misserfolg. Wenn der Test fehlschlägt, überprüfen/aktualisieren Sie die Authentifizierungsdaten und versuchen Sie es erneut.

5.4.2 Konfigurieren eines dedizierten Benutzerkontos für Exchange Server 2003

Wenn GFI MailEssentials in einer DMZ installiert ist, sollten Sie aus Sicherheitsgründen unbedingt ein dezidiertes Benutzerkonto erstellen um E-Mails aus öffentlichen Ordnern zu laden und zu scannen. Die Benutzer haben Zugriff auf die GFI-Spam-Ordner.

1. Erstellen Sie einen neuen Active Directory (AD-) Benutzer mit Poweruser-Rechten.

2. Öffnen Sie im Microsoft Exchange System Manager den Knoten **Ordner** ► **Öffentliche Ordner**.

3. Klicken Sie mit der rechten Maustaste auf den öffentlichen Ordner **Anti-Spam folders** und dann auf **Eigenschaften**.

4. Klicken Sie auf die Registerkarte **Berechtigungen** und wählen Sie **Client-Berechtigungen** aus.

5. Klicken Sie auf **Hinzufügen** …, wählen Sie die Option "Neuer Benutzer" und klicken Sie auf **OK**.

6. Wählen Sie die Option "Neuer Benutzer" aus der Liste der Client-Berechtigungen und aus der angezeigten Liste die Rolle 'Besitzer'. Achten Sie darauf, dass alle Kontrollkästchen aktiviert sind und die Radioschaltflächen auf **Alle** eingestellt sind.

7. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

8. Klicken Sie im Microsoft Exchange System Manager mit der rechten Maustaste auf **Anti-Spam folders** und dann auf **Alle Aufgaben** ► **Einstellungen übernehmen**.

9. Klicken Sie auf die Option **Ordnerrechte** und dann auf **OK**.

10. Definieren Sie die Authentifizierungsdaten des in Schritt 1 erstellten Poweruser-Kontos und testen Sie die Konfiguration um sicherzugehen, dass die Rechte richtig definiert sind.

5.4.3 Konfigurieren eines dezidierten Benutzerkontos für Exchange Server 2007/2010

Wenn Sie ein dezidiertes Benutzerkonto konfigurieren, das E-Mails aus den öffentlichen GFI-Spam-Ordnern laden soll, muss der Benutzer Zugriffsrechte als 'Besitzer' der öffentlichen GFI-Anti-Spam folders haben.

1. Erstellen Sie einen neuen Active Directory (AD) (Power-) User.

2. Melden Sie sich bei Microsoft Exchange Server mit Administratorrechten an.

3. Öffnen Sie die 'Microsoft Exchange Manager Shell' und geben Sie folgenden Befehl ein:

```
Get-PublicFolder -Identity "\GFI Anti-Spam Folders" -Recurse | ForEach-Object {Add-PublicFolderClientPermission -Identity $_.Identity -User "BENUTZERNAME" -AccessRights owner -Server "SERVERNAME"}
```

4. Ändern Sie "BENUTZERNAME" und "SERVERNAME" entsprechend dem betreffenden Active Directory-Benutzer.

» Beispiel:

```
Get-PublicFolder -Identity "\GFI Anti-Spam Folders" -Recurse | ForEach-Object {Add-PublicFolderClientPermission -Identity $_.Identity -User "mesuser" -AccessRights owner -Server "exch07"}
```

5.4.4 Verbergen von Benutzermitteilungen in GFI-Spam-Ordnern

Aus Sicherheits- und Datenschutzgründen sollten Sie die Benutzernachrichten verbergen, die sich

in einem GFI-Spam-Ordner befinden. So können die Benutzer Nachrichten an die Ordner senden, aber die vorhandenen Nachrichten nicht sehen (nicht einmal die, die sie selbst gesendet haben). Um Benutzerrechte zu konfigurieren und Nachrichten für unbefugte Benutzer zu verbergen, gehen Sie wie folgt vor:

Microsoft Exchange 2003

1. Öffnen Sie im Microsoft Exchange System Manager den Knoten **Ordner ► Öffentliche Ordner.**

2. Klicken Sie mit der rechten Maustaste auf den öffentlichen Ordner **Anti-Spam folders** und dann auf **Eigenschaften**.

3. Klicken Sie auf die Registerkarte **Berechtigungen** und dann auf **Client-Berechtigungen**.

4. Klicken Sie auf **Hinzufügen…** und wählen Sie den Benutzer/die Gruppe aus, deren Nachrichten Sie verbergen wollen, und klicken Sie dann auf **OK**.

5. Wählen Sie den zuvor konfigurierten Benutzer/die Benutzergruppe für die Client-Berechtigungsliste aus und stellen Sie als Benutzerrolle **Teilnehmen** ein.

6. Achten Sie darauf, dass nur das Kontrollkästchen **Elemente erstellen** ausgewählt ist und die Radioschaltflächen auf **Keine** eingestellt sind.

7. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

8. Klicken Sie im Microsoft Exchange System Manager mit der rechten Maustaste auf **Anti-Spam folders** und dann auf **Alle Aufgaben ► Einstellungen übernehmen**.

9. Aktivieren Sie das Kontrollkästchen **Ordnerrechte** und klicken Sie auf **OK**.

Microsoft Exchange 2007

1. Geben Sie im Microsoft Exchange-Verwaltungsshell folgenden Befehl ein:

```
ReplaceUserPermissionOnPFRecursive.ps1 -Server "server" -TopPublicFolder
"\'GFI AntiSpam Folders'" -User "Default" -Permissions Contributor
```

Ersetzen Sie „server“ mit dem vollständigen Computernamen.

2. Geben Sie bei Aufforderung **y** ein, um die Berechtigungen für jeden Ordner zu bestätigen.

Dieser Befehl legt die Standardberechtigungen für die öffentlichen Ordner von GFI MailEssentials fest. Benutzer können dort E-Mails abspeichern, jedoch keine Einträge anzeigen oder ändern. Standardmäßig sind Administratoren die Benutzer der öffentlichen Ordner und können Einträge anzeigen und ändern. Weitere Informationen zu Berechtigungen für öffentliche Ordner finden Sie unter:

http://technet.microsoft.com/en-us/library/bb310789.aspx

Microsoft Exchange 2010

1. Ändern Sie im Microsoft Exchange-Verwaltungsshell den Ordner für Microsoft Exchange-Skripts, der sich im Installationsordner von Microsoft Exchange befindet. Falls Microsoft Exchange auf dem Standardpfad installiert wurde, befindet sich der Skriptordner unter:

C:\Program Files\Microsoft\Exchange Server\V14\Scripts\

2. Geben Sie folgenden Befehl ein:

```
ReplaceUserPermissionOnPFRecursive.ps1 -Server "server" -TopPublicFolder
"\GFI AntiSpam Folders" -User "Default" -Permissions Contributor
```

Ersetzen Sie „server“ mit dem vollständigen Computernamen.

Dieser Befehl legt die Standardberechtigungen für die öffentlichen Ordner von GFI MailEssentials fest. Benutzer können dort E-Mails abspeichern, jedoch keine Einträge anzeigen oder ändern. Standardmäßig sind Administratoren die Benutzer der öffentlichen Ordner und können Einträge anzeigen und ändern. Weitere Informationen zu Berechtigungen für öffentliche Ordner finden Sie unter:

http://technet.microsoft.com/en-us/library/bb310789(EXCHG.140).aspx

5.4.5 Konfiguration zum Konfiguration zum Scannen öffentlicher Ordner für Lotus Domino Server

Schritt 1: Erstellen Sie eine neue Datenbank, in der Sie die öffentlichen Ordner von GFI MailEssentials speichern wollen.

1. Klicken Sie in IBM Domino Administrator auf **Datei** ► **Datenbank** ► **Neu**.

2. Geben Sie für die neue Datenbank folgende Details ein:

» Server: <Die Details Ihres Domino Servers>

» Titel: Öffentlicher Order

» Dateiname: Public-F.nsf

» Wählen Sie als Vorlage für die neue Datenbank 'Mail (R7)'.

3. Klicken Sie auf **OK** um die Datenbank zu erstellen.

Schritt 2: Konvertieren Sie das Datenbankformat der neu erstellten Datenbank.

1. Klicken Sie in der Lotus Domino Server Console, und geben Sie folgenden Befehl ein:

```
Load Convert -e -h <Datenbank Dateiname>
```

» Beispiel:

```
Load Convert -e -h Public-F.nsf
```

Schritt 3: Erstellen Sie eine neue Mail-In-Datenbank:

Sie müssen ein neues Postfach erstellen, damit Sie den neuen öffentlichen Ordner von GFI MailEssentials speichern können.

1. Wählen Sie im IBM Domino Administrator die Registerkarte **Personen und Gruppen** und klicken Sie auf **Mail-In-Datenbanken und Ressourcen**.

2. Klicken Sie auf **Mail-In-Datenbank hinzufügen** und geben Sie die neue Mail-In-Datenbank wie folgt ein:

» Name der Mail-In-Datenbank: Public Folders

» Beschreibung: GFI MailEssentials-Postfach

» Internetadresse: <public@<yourdomain>.com>

» Internetnachricht: 'Keine Präferenz'

» Eingehende E-Mail verschlüsseln: 'Nein'

» Domäne: <yourdomain>

» Server: <Name Ihres Domino Servers>

» Dateiname: 'Public-F.nsf'

HINWEIS: Sie müssen mit der oben erstellten Mail-In-Datenbank einen Benutzer verknüpfen. Dieses Konto wird vom GFI MailEssentials-Server für den Verbindungsaufbau mit Lotus Domino-Server verwendet.

Schritt 4: Konfigurieren Sie GFI MailEssentials.

Definieren Sie den gemeinsamen Namespace, der beim Verbindungsaufbau mit dem Lotus Domino IMAP-Service verwendet wird:

1. Klicken Sie auf **Start** ► **Ausführen** und geben Sie **Regedit** ein.

2. Suchen Sie folgenden Registrierschlüssel:

```
<HKEY_LOCAL_MACHINE\SOFTWARE\GFI\ME15\Attendant\rpfolders:8\>
```

3. Erstellen Sie folgende Schlüssel:

• Name: 'FolderDelimiter'	• Name: 'SharedNamespace'
• Typ: STRING	• Typ: STRING
• Wert: ‘\\’	• Wert: <Präfixbezeichnung des öffentlichen Ordners\Name der neuen Mail-In-Datenbank\>

Laden Sie die Werte für den Schlüssel 'sharednamespace' wie folgt:

» Präfix für öffentlichen Ordner, Name

1. Klicken Sie in IBM Domino Administrator auf die Registerkarte **Konfiguration**.

2. Klicken Sie auf **Server ▶ Konfigurationen,** dann auf den Domino Server sowie auf **Konfiguration bearbeiten.**

3. Wählen Sie auf der Registerkarte **IMAP** die Registerkarte **Öffentliche Ordner und Ordner anderer Benutzer**. Den 'Public Folder Prefix' finden Sie im Abschnitt "Public Folder".

Name der Mail-In-Datenbank

1. Wählen Sie in IBM Domino Administrator die Registerkarte **Personen und Gruppen**.

2. Klicken Sie auf den Knoten **Mail-In-Datenbanken und Ressourcen**. Der Name der neuen Mail-In-Datenbank wird im rechten Feld angezeigt.

Schritt 5: Starten Sie den IMAP-Service auf Domino Server neu.

1. Öffnen Sie die Konsole von Lotus Notes.

2. Geben Sie 'tell imap quit' ein und warten Sie, bis die Aufgabe abgeschlossen ist.

3. Sobald diese Schritte abgeschlossen sind, geben Sie 'load imap'ein.

Schritt 6: Konfigurieren Sie GFI MailEssentials.

Konfigurieren Sie die Scan-Eigenschaften für den öffentlichen Ordner von GFI MailEssentials. 1. Klicken Sie in der Konfiguration von GFI MailEssentials auf den Knoten **Anti-Spam** und dann auf **Eigenschaften.**

2. Wählen Sie die Registerkarte **Scannen öffentlicher Ordner** aus und geben Sie folgende Werte ein:

» Server: <IP-Adresse des Domino Server>

» Port: 143 (Standard)

» Benutzername: Den mit der Mail-In-Datenbank verknüpften Benutzernamen

» Kennwort: Benutzerkennwort

3. Testen Sie die Konfiguration, indem Sie auf die Schaltfläche **Testen** klicken und anschließend auf **Jetzt scannen** um die öffentlichen Ordner zu erzeugen.

Schritt 7: Kontrollieren Sie, ob die öffentlichen Ordner erstellt werden.

Prüfen Sie mit Telnet, ob die öffentlichen Ordner erfolgreich erstellt wurden:

1. Öffnen Sie auf dem Computer mit GFI MailEssentials eine Befehlszeile.

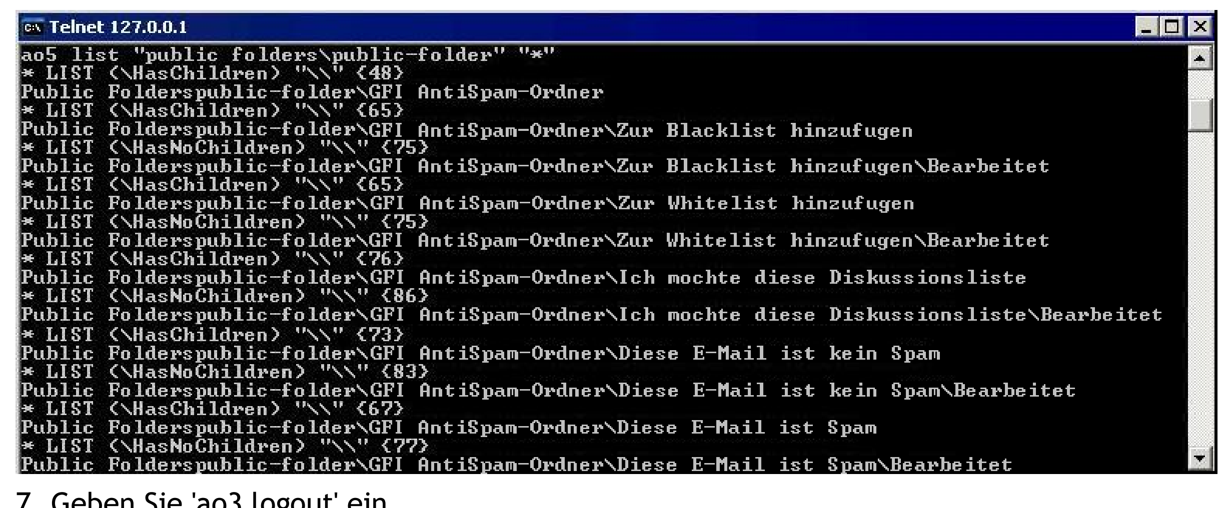
2. Geben Sie ein: 'telnet'

3. Geben Sie ein: 'Open <*IP-ADRESSE*> 143'

4. Geben Sie ein: 'ao1 login <public@yourdomain.com> <Kennwort>'

5. Geben Sie ein: 'ao5 list “<Präfix des öffentlichen Orders\Name der neuen Mail-In-Datenbank\>” “*”.

6. Die Ausgabe des oben erwähnten Befehls sollte die öffentlichen Ordner wie in dem folgenden Bild anzeigen:



7. Geben Sie 'ao3 logout' ein.

HINWEIS: Entfernen Sie mit Lotus Notes Designer unerwünschte Ansichten und Formulare aus der zuvor erstellten Datenbank.

6 Anpassen weiterer Funktionen

6.1 Haftungsausschluss

Haftungsausschlüsse sind Standardtexte, die am Beginn oder am Ende ausgehender E-Mails aus juristischen oder Marketinggründen eingefügt werden. Sie helfen den Unternehmen, sich gegen Klagen zu schützen, die mit dem Inhalt einer E-Mail zusammenhängen, und ergänzen Beschreibungen über die angebotenen Produkte und Dienstleistungen.

6.1.1 Konfiguration von Haftungsausschlüssen

1. Klicken Sie mit der rechten Maustaste auf den Knoten **E-Mail-Verwaltung ► Haftungsausschluss** und dann auf **Neu ► Haftungsausschluss**.

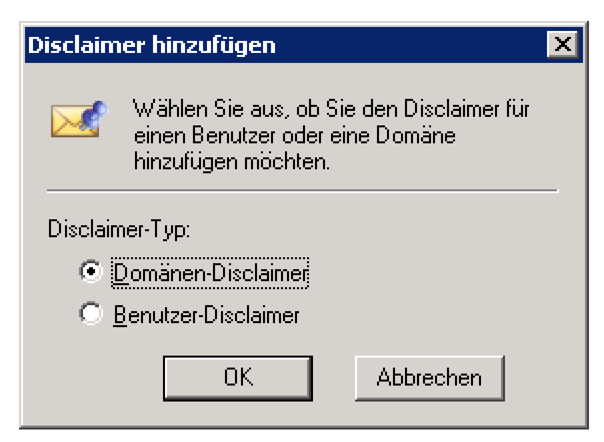


Bild 56 - Auswahl eines Haftungsausschlusses für eine Domäne oder einen Benutzer

2. Wählen Sie:

- **Domäne** - Wählen Sie die Domäne aus der Liste der konfigurierten Domäne. Alle von dieser Domäne versendeten E-Mails enthalten den ergänzten Haftungsausschluss
- **Benutzer** - Geben Sie an, bei welchem Benutzer oder bei welcher Benutzergruppe der Haftungsausschluss bei ausgehenden E-Mails ergänzt werden soll. Wenn GFI MailEssentials im Active Directory-Modus arbeitet, entnehmen Sie die Benutzer bzw. die Benutzergruppen direkt aus der Active Directory; anderenfalls geben Sie die SMTP-E-Mail-Adresse des Benutzers an.

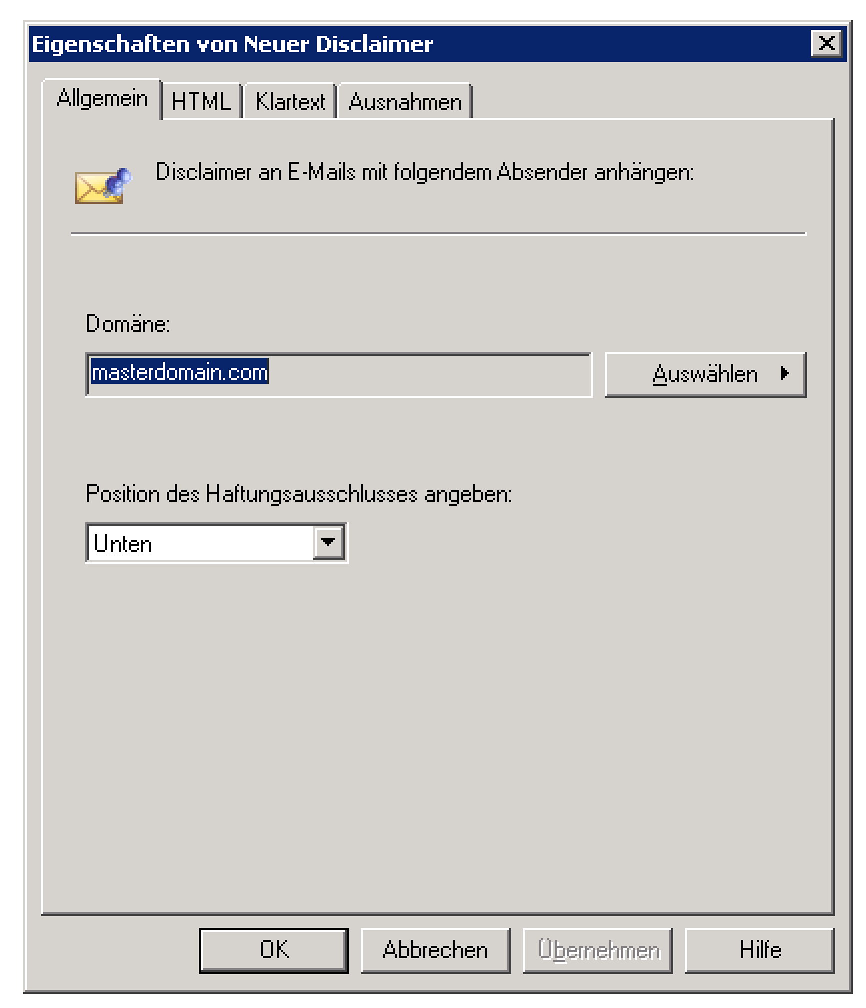


Bild 57 - Neuer Haftungsausschluss - Allgemeine Eigenschaften

3. Klicken Sie in der Registerkarte **Allgemein** auf **Auswählen**, um die Domäne oder den Benutzer zu ändern. Klicken Sie auf **oben** oder **unten,** um festzulegen, ob der Haftungsausschluss am Anfang oder Ende der E-Mail eingefügt werden soll.

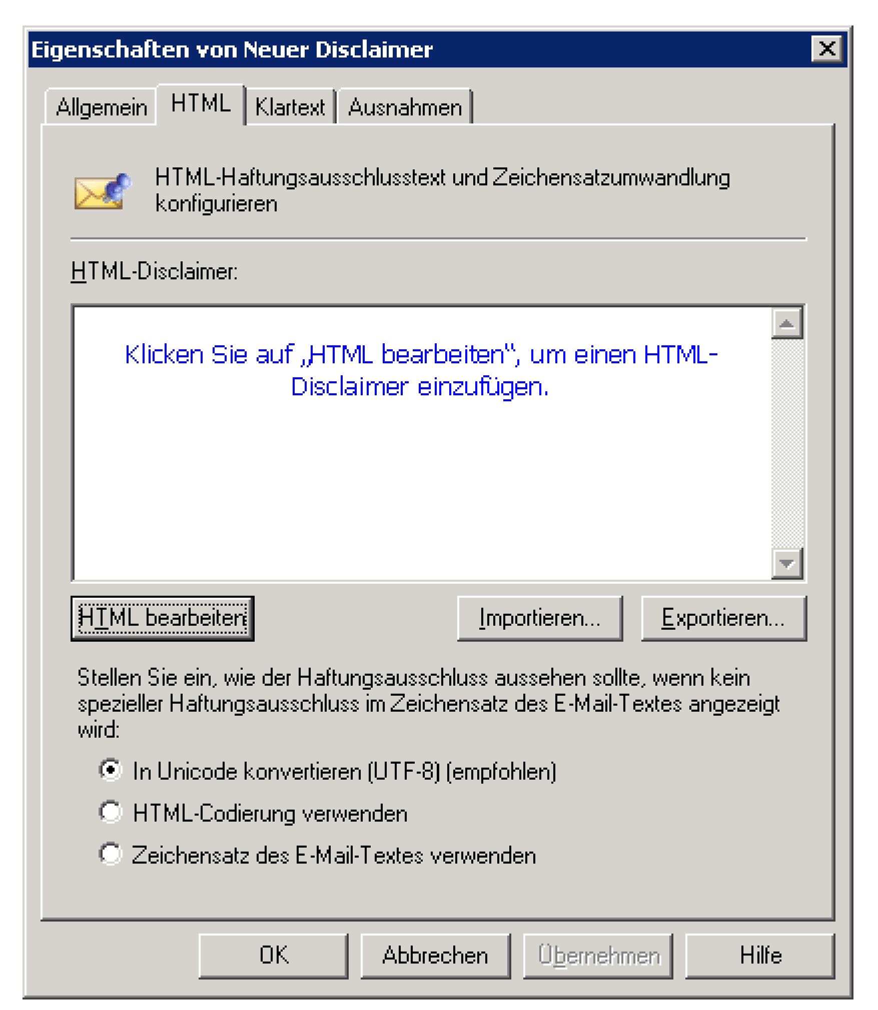


Bild 58 - HTML-Haftungsausschluss

4. Klicken Sie zum Hinzufügen eines Haftungsausschlusses im 'HTML-Format' auf die Registerkarte HTML. Klicken Sie auf **HTML bearbeiten**, um den Editor für den HTML-Haftungsausschluss zu öffnen und den Text für den HTML-Haftungsausschluss zu bearbeiten.

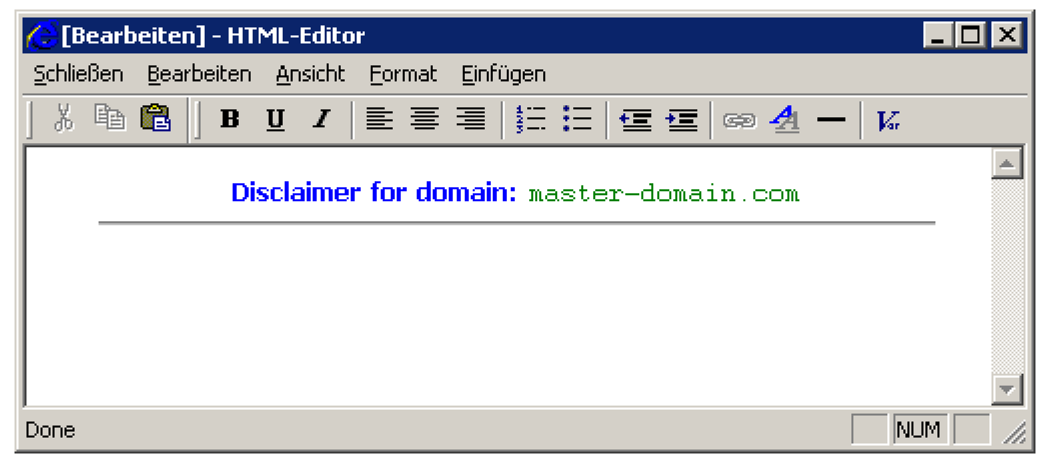


Bild 59 - HTML-Editor für den Haftungsausschluss

5. Um Variable in den Disclaimer einzufügen, öffnen Sie **Einfügen ► Variable…**. Die Variablen, die hinzugefügt werden können, sind E-Mail- oder Active Directory-Felder. Wählen Sie die gewünschte Variable, und klicken Sie auf **OK**.

HINWEIS 1: Die Variablen für den Anzeigenamen und die E-Mail-Adresse des Empfängers werden nur dann eingesetzt, wenn die E-Mail lediglich an einen einzelnen Empfänger geschickt wird. Beim Verschicken der E-Mail an mehrere Empfänger wird die Variable automatisch mit dem Eintrag „Empfänger“ ersetzt.

HINWEIS 2: Active Directory-Felder können nur verwendet werden, falls GFI MailEssentials nicht auf dem Perimeter-SMTP-Server installiert ist.

6. Klicken Sie auf **Schließen**, wenn die Bearbeitung des HTML-Disclaimers abgeschlossen ist.

7. Geben Sie die Codierung für den HTML-Haftungsausschluss an, wenn der Zeichensatz für den E-Mail-Text nicht HTML ist:

- **HTML-Codierung verwenden** - definieren Sie mit der HTML-Codierung die Zeichensätze für den E-Mail-Text und den Haftungsausschluss. Diese Option wird empfohlen.
- **In Unicode konvertieren** - konvertiert den E-Mail-Text und den Haftungsausschluss in Unicode, so dass beide Teile richtig angezeigt werden.
- **Zeichensatz des E-Mail-Textes verwenden** - der Haftungsausschluss wird in den Zeichensatz des E-Mail-Textes konvertiert.

  Hinweis: Ist diese Option ausgewählt, wird eventuell nicht der ganze Text des Haftungsausschlusses richtig angezeigt.

8. Importieren oder exportieren Sie einen HTML-Haftungsausschluss mit den Schaltflächen **Importieren** bzw. **Exportieren**.

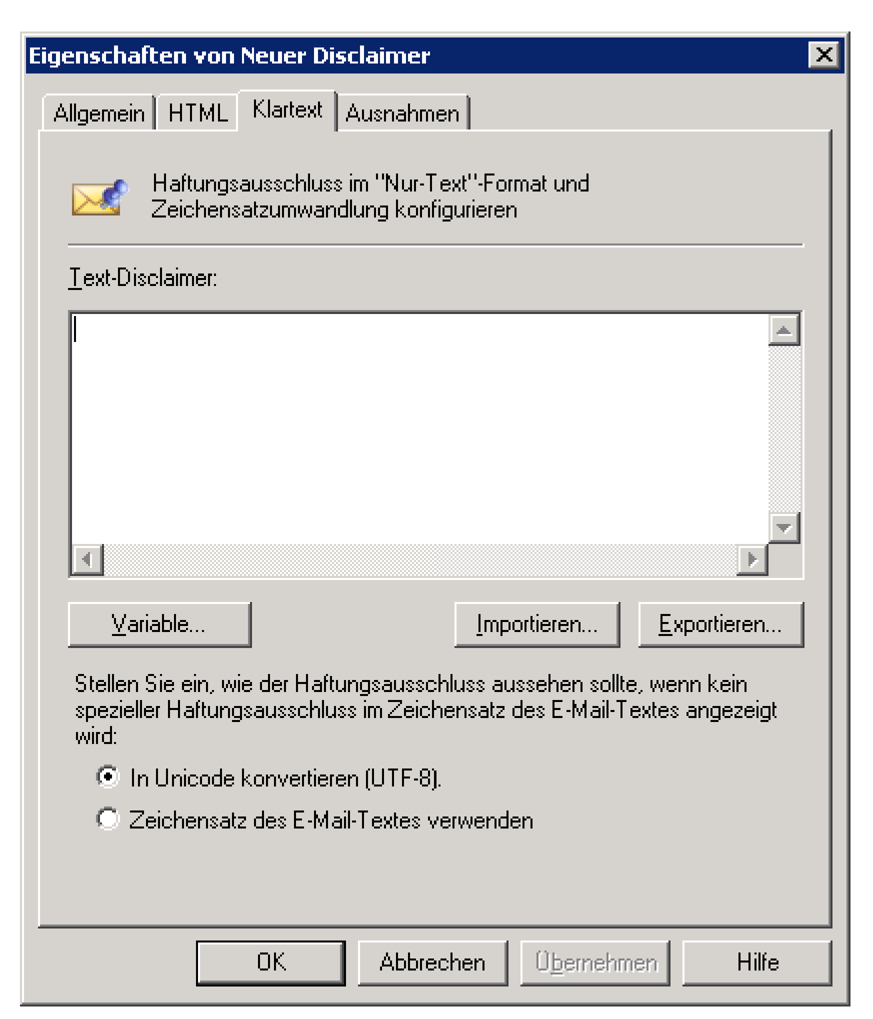


Bild 60 - 'Nur-Text'-Haftungsausschluss

9. Eine Textversion Ihres Haftungsausschlusses kann auch in reinen Text-E-Mails eingefügt werden. Klicken Sie auf die Registerkarte **Nur-Text** und fügen Sie den Text direkt in das Feld **Text Haftungsausschluss** ein.

10. Um Variable in den Haftungsausschlusses einzufügen, klicken Sie auf **Variable…**. Die Variablen, die hinzugefügt werden können, sind E-Mail- (Absendername, E-Mail-Adresse des Empfänger usw.) oder Active Directory-Felder (Name, Titel, Telefonnummern usw.). Wählen Sie die gewünschte Variable, und klicken Sie auf **OK**.

HINWEIS 1: Die Variablen für den Anzeigenamen und die E-Mail-Adresse des Empfängers werden nur dann eingesetzt, wenn die E-Mail lediglich an einen einzelnen Empfänger geschickt wird. Beim Verschicken der E-Mail an mehrere Empfänger wird die Variable automatisch mit dem Eintrag „Empfänger“ ersetzt.

HINWEIS 2: Active Directory-Felder können nur verwendet werden, falls GFI MailEssentials nicht auf dem Perimeter-SMTP-Server installiert ist.

11. Geben Sie die Codierung für den Haftungsausschluss im 'Nur-Text' Format an, wenn der Zeichensatz des E-Mail-Textes nicht das 'Nur-Text'-Format ist:

» **In Unicode konvertieren** - konvertiert E-Mail-Text und Haftungsausschluss in Unicode, so dass beide Teile richtig angezeigt werden.

» **Zeichensatz des E-Mail-Textes verwenden** - der Haftungsausschluss wird in den Zeichensatz des E-Mail-Textes konvertiert.

  Hinweis: Ist diese Option ausgewählt, wird eventuell nicht der ganze Text des Haftungsausschlusses richtig angezeigt.

12. Importieren oder exportieren Sie einen Haftungsausschluss im 'Nur-Text'-Format mit den Schaltflächen **Importieren** und **Exportieren**.

13. Wählen Sie die Registerkarte **Ausnahmen**, um Absender oder Empfänger festzulegen, auf die

dieser Disclaimer nicht angewendet werden soll. Klicken Sie auf **Hinzufügen**, und geben Sie **Benutzer** oder **E-Mail-Adressen** an, die ausgeschlossen werden sollen.

HINWEIS: Alle Empfänger müssen in die Ausschlussliste aufgenommen werden, damit E-Mails kein Disclaimer hinzugefügt wird.

14. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Der neu erstellte Haftungsausschluss wird auf der rechten Seite der Konfigurationskonsole von GFI MailEssentials angezeigt. Um dem neuen Haftungsausschluss einen aussagefähigen Namen zu geben, klicken Sie mit der rechten Maustaste auf den Haftungsausschluss und dann auf **Umbenennen**.

6.1.2 Aktivieren und Deaktivieren von Haftungsausschlüssen

Standardmäßig werden neue Haftungsausschlüsse automatisch aktiviert. So aktivieren oder deaktivieren Sie einen Haftungsausschluss:

1. Klicken Sie mit der rechten Maustaste auf den zu deaktivierenden Haftungsausschluss.

2. Klicken Sie auf **Deaktivieren** oder **Aktivieren** um die gewünschte Aktion auszuführen.

6.2 Automatische Antworten

Die Funktion "Automatische Antwort" erlaubt einen Versand automatischer Antworten an bestimmte eingehende E-Mails. Für jede E-Mail-Adresse bzw. Betreffzeile können Sie eine andere automatische Antwort definieren. Sie können in einer automatischen Antwort mit Variablen eine E-Mail personalisieren.

Wichtige Hinweise

1. Fügen Sie keinen Nachrichtentext ein, der mehr als 30 bis 40 Zeichen pro Zeile mit Zeilensprung enthält. Einige ältere E-Mail-Server schneiden Zeilen bei 30 bis 40 Zeichen ab.

6.2.1 Konfiguration von automatischen Antworten

1. Klicken Sie mit der rechten Maustaste auf den Knoten **E-Mail-Verwaltung ► Automatische Antwort** und dann auf **Neu ► Automatische Antwort**.

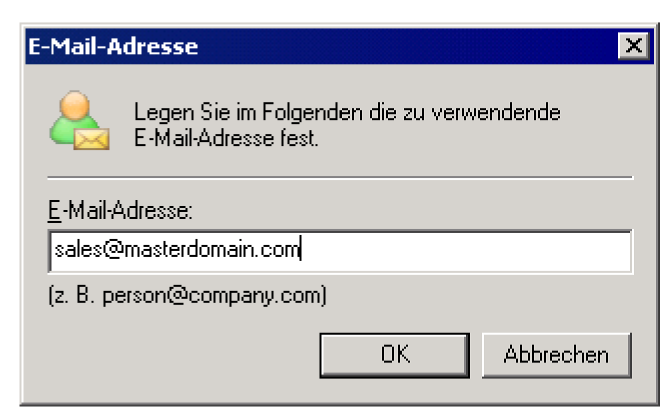


Bild 61 - Erstellen einer neuen automatischen Antwor

2. Geben Sie die E-Mail-Adresse ein, die Sie für die automatische Antwort konfigurieren wollen, und klicken Sie auf **OK**.

» **Beispiel** - Wenn Sie 'sales@master-Domäne.com' angeben, werden an diese E-Mail-Adresse gesendete E-Mails automatisch beantwortet.

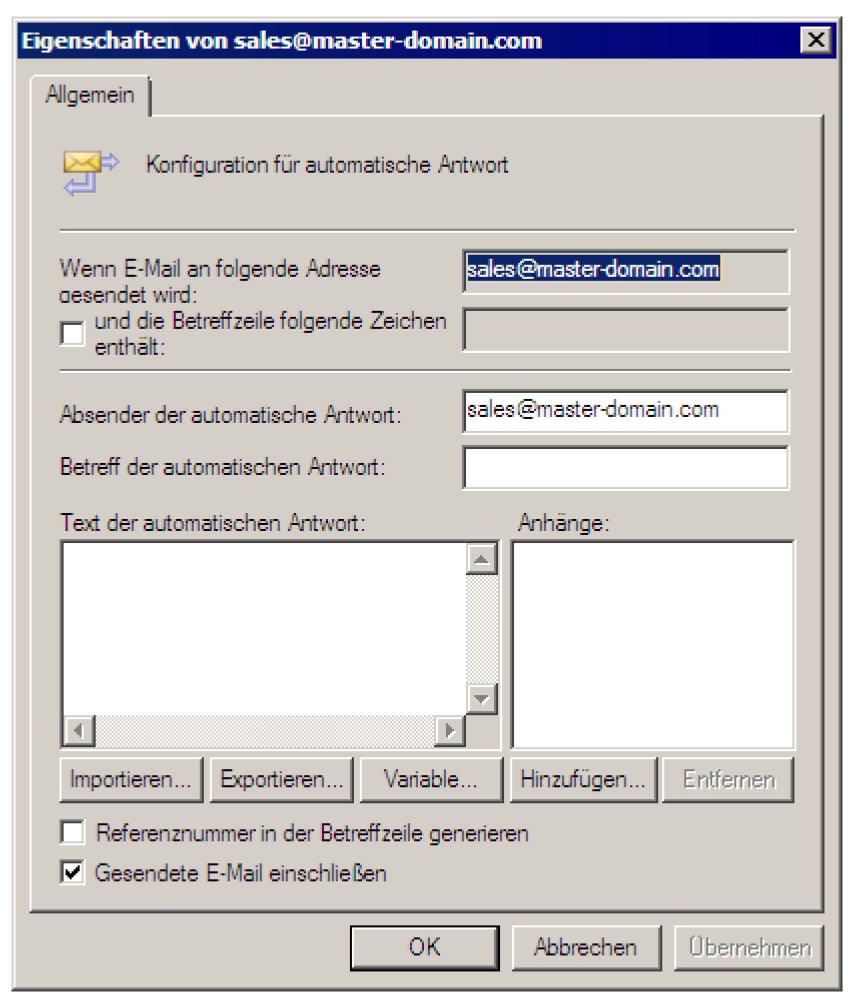


Bild 62 - Automatische Antwort - Eigenschaften

3. Aktivieren Sie das Kontrollkästchen **Betreff enthält** um automatische Antworten für E-Mails zu aktivieren, die in der Betreffzeile einen bestimmten Text enthalten.

4. Definieren Sie in dem Feld **Automatische Antwort von:** eine E-Mail-Adresse, wenn eine automatische Antwort von einer anderen E-Mail-Adresse als der E-Mail-Adresse erfolgen soll, an die die eingehende E-Mail gesendet wurde.

5. Geben Sie in dem Feld **Betreff automatische Antwort** den Betreff für die E-Mail mit der automatischen Antwort an.

6. Definieren Sie in dem Bearbeitungsfeld **Automatische Antwort - Text** den Text, der in der E-Mail mit der automatischen Antwort angezeigt werden soll.

HINWEIS: Importieren Sie den Text für die automatische Antwort aus einer Textdatei mit der Schaltfläche **Importieren ...**.

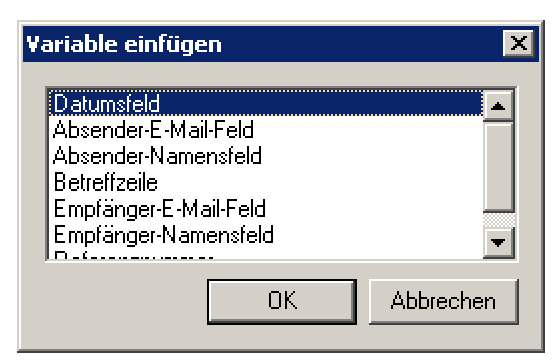


Bild 63 - Der Dialog "Variablen"

7. Klicken Sie auf **Variable…** um die automatischen Antworten mit Variablen zu personalisieren. Klicken Sie auf das Feld für die Variable um die Variable einzufügen und anschließend auf **OK.** Verfügbare Variablen sind:

1. **Datumsfeld** - setzt das Sendedatum der E-Mail ein.

2. **Absender-E-Mail-Feld** - setzt die E-Mail-Adresse des Absenders ein.

3. **Absender-Namensfeld** - setzt den angezeigten Namen des Absenders ein.

4. **Betreff-Feld** - setzt den Betreff für die E-Mail ein.

5. **Empfänger-E-Mail-Feld** - fügt die E-Mail-Adresse des Empfängers ein.

6. **Empfänger-Namensfeld** - fügt den angezeigten Namen des Empfängers ein.

7. **Referenznummer** - fügt Referenznummern ein (sofern erzeugt).

8. Klicken Sie auf **Hinzufügen...** und dann auf Dateianhänge, die mit der automatischen Antwort-E-Mail versendet werden sollen. Entfernen Sie Dateianhänge mit der Schaltfläche **Entfernen**.

9. Klicken Sie auf die Option **Gesendete E-Mail einfügen** um die eingegangene E-Mail in der automatischen Antwort zu zitieren.

10. Klicken Sie auf **Referenznummer in Betreffzeile erzeugen** um in den automatischen Antworten Referenznummern zu erzeugen.

HINWEIS: Mit dieser Funktion können Kunden beispielsweise eine Referenznummer angeben, mit der Mitarbeiter E-Mails besser zurückverfolgen können.

11. Klicken Sie auf **OK** um die Einstellungen zu übernehmen.

Standardmäßig werden Referenznummern in folgendem Format erzeugt:

`ME_JJMMTT_nnnnnn`

Bedeutung:

- **ME -** GFI MailEssentials-Tag.
- **JJMMTT -** Datum im Format Jahr, Monat und Tag.
- **nnnnnn -** automatisch erzeugte Referenznummer.

6.3 Listenservers

Listenserver unterstützen die Erstellung von zwei Arten von Verteilerlisten:

1. Newsletter-Abonnenten-Liste - Genutzt wird diese Funktion zum Erstellen von Abonnementlisten für Firmen- oder Produkt-Newsletter, bei denen sich Benutzer eintragen oder austragen können.

2. Diskussionsliste - Mit dieser Option können Gruppen von Personen Diskussionen per E-Mail führen, wobei jedes Mitglied der Liste jede E-Mail empfängt, die ein Benutzer an die Liste sendet.

6.3.1 Erstellen eines Newsletters oder einer Diskussionsliste

1. Klicken Sie mit der rechten Maustaste in der Konfigurationskonsole von GFI MailEssentials auf **E-Mail-Verwaltung ► Listenserver** und anschließend auf **Neu ► Newsletter** oder **Diskussionsliste.**

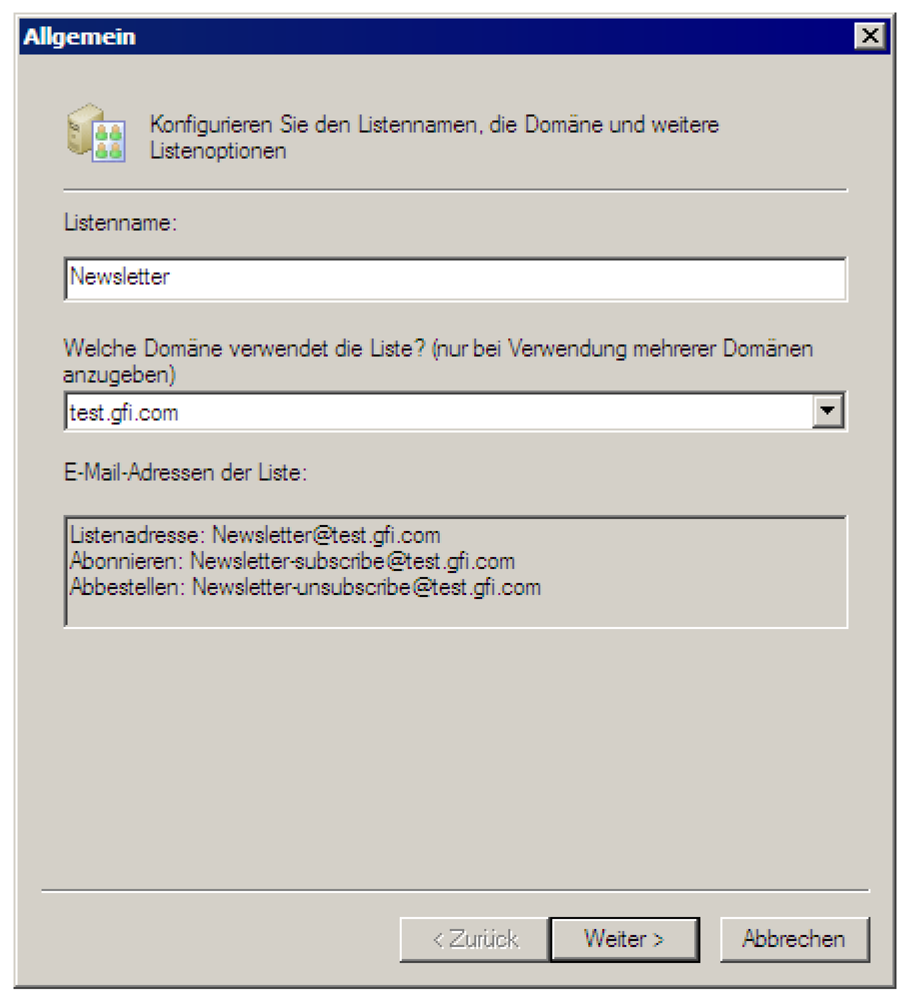


Bild 64 - Erstellen einer neuen Newsletter Newsletter-Liste

2. Geben Sie in dem Feld **Listenname:** einen Namen für die neue Liste ein und wählen Sie eine Domäne für die Liste aus (nur wenn Sie mehrere Domänen besitzen). Klicken Sie auf **Weiter** um fortzufahren.

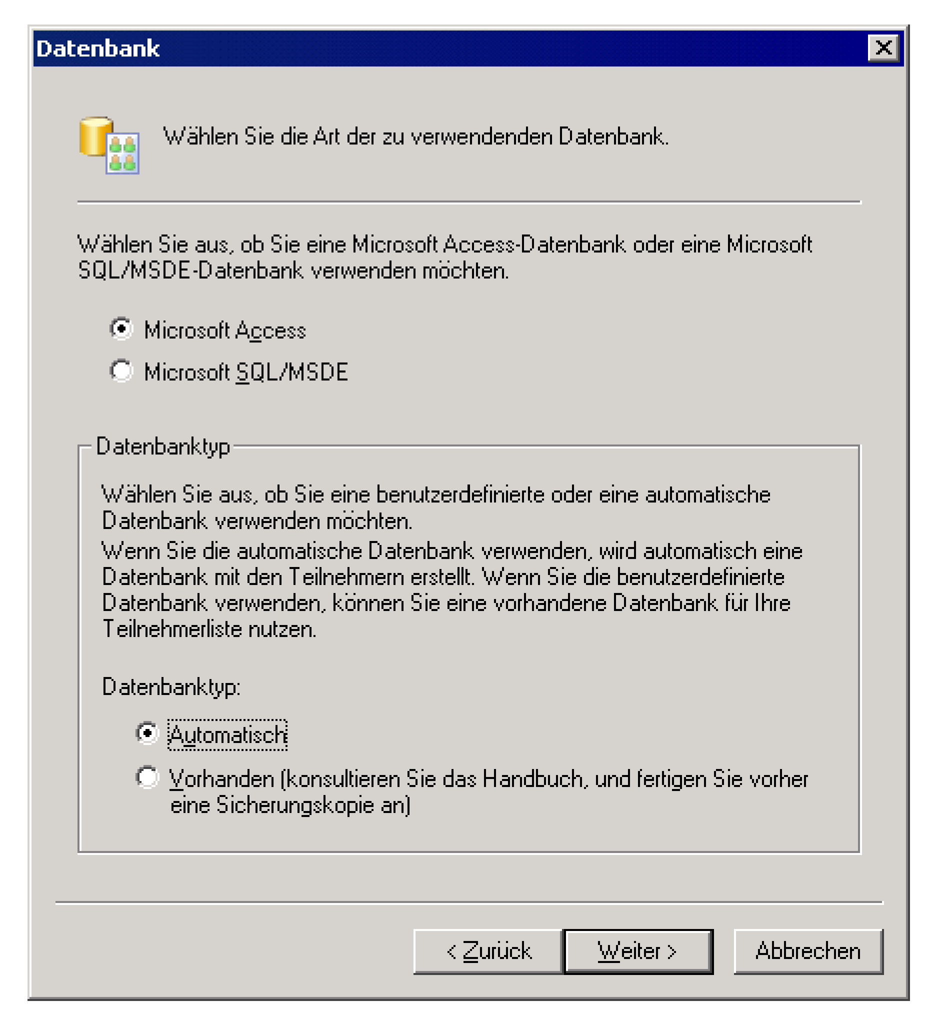


Bild 65 - Definition des Datenbank-Backends

3. Wählen Sie **Microsoft Access** oder **Microsoft SQL Server/MSDE** als Datenbank aus und in der Gruppe **Datenbanktyp**, ob GFI MailEssentials eine neue Datenbank erstellen oder eine Verbindung mit einer vorhandenen Datenbank aufbauen soll. Klicken Sie auf Weiterum fortzufahren.

HINWEIS 1: Für kleinere Listen mit bis zu 5.000 Mitgliedern können Sie Microsoft Access als Backend verwenden.

HINWEIS 2: Um eine neue Datenbank zu erstellen, klicken Sie auf die Option **Automatisch**.

4. Konfigurieren Sie den ausgewählten Datenbanktyp zur Speicherung der Newsletter-/Diskussions-Listen. Die verfügbaren Optionen sind:

DATENBANKTYP	DATENBANKEINSTELLUNGEN
Microsoft Access mit der Option "Automatisch"	Geben Sie in dem Bearbeitungsfeld Datei an, wo die neue Datenbank gespeichert ist.
Microsoft Access mit der Option "Vorhanden"	Geben Sie in dem Feld Datei den Pfad zu Ihrer vorhandenen Microsoft Access-Datenbank ein, die die Newsletter-/Diskussionsabonnenten enthält. Klicken Sie in der Dropdown-Liste Tabelle auf die Tabelle, in der die Abonnentenliste gespeichert ist.
Microsoft SQL Server mit Option "Automatisch"	Geben Sie den Namen des SQL-Servers, die Anmeldedaten und die Datenbank zur Speicherung der Newsletter-/Diskussionsabonnentenliste an.
Microsoft SQL mit der Option "Vorhanden"	Geben Sie den Namen des SQL-Servers und die Anmeldedaten ein und wählen Sie die Datenbank und die Datentabelle, in der die Abonnenten gespeichert werden.

5. Klicken Sie bei allen Datenbanktypen mit der Option **Automatisch** zum Abschluss des Assistenten auf die Schaltfläche **Fertigstellen** oder auf die Schaltfläche **Weiter** um mit dem

Setup fortzufahren.

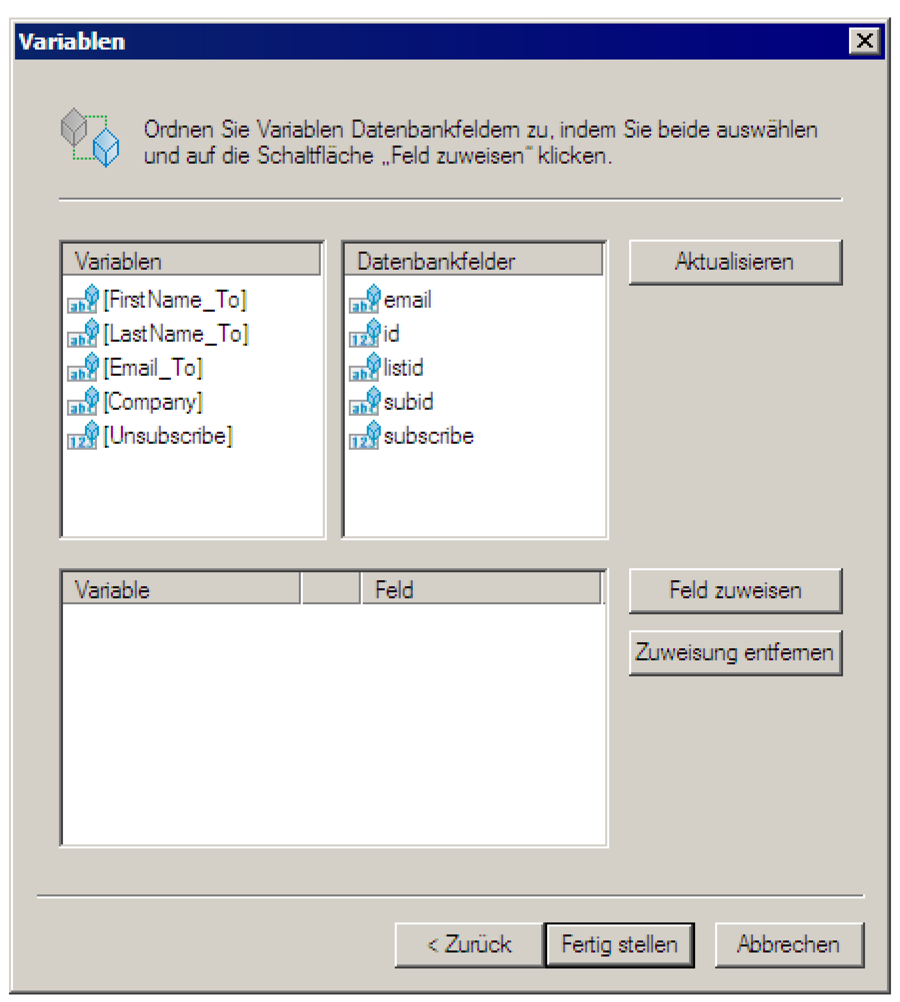


Bild 66 - Zuordnung benutzerdefinierter Felder

6. Wählen Sie eine Variable aus der Liste **Variablen** und klicken Sie auf die entsprechende Option **Datenbankfelder** sowie auf die Schaltfläche **Feld zuordnen** um die benötigten Felder den benutzerdefinierten Feldern in der Datenbank zuzuordnen. Klicken Sie auf **Fertigstellen** um Ihre Konfiguration zu übernehmen. Folgende Felder werden zugeordnet:

- **[Email_To]** - Zuordnung eines Text-String-Felds mit der E-Mail-Adresse eines Abonnenten.
- **[Unsubscribe]** - Zuordnung zu einem Feld mit einer Ganzzahl oder einem booleschen Wert, aus der/dem hervorgeht, ob der Benutzer in der Liste ein- oder ausgetragen ist.
- **[FirstName_To]** - Zuordnung eines Text-String-Felds mit dem Vornamen eines Abonnenten.
- **[LastName_To]** - Zuordnung eines Text-String-Felds mit dem Nachnamen eines Abonnenten.
- **[Company]** - Zuordnung eines Text-String-Felds mit dem Namen der Firma eines Abonnenten.

6.3.2 Konfigurieren erweiterter Eigenschaften für Newsletter/Diskussionslisten

Sobald Sie eine neue Liste erstellt haben, können Sie weitere Optionen konfigurieren, beispielsweise Elemente und Verhalten der Liste benutzerspezifisch anpassen.

Erstellen einer benutzerdefinierten Fußzeile für die Liste

Eine benutzerspezifische Fußzeile im HTML- oder Textformat konfigurieren. Dabei wird jeder E-Mail eine Fußzeile hinzugefügt.

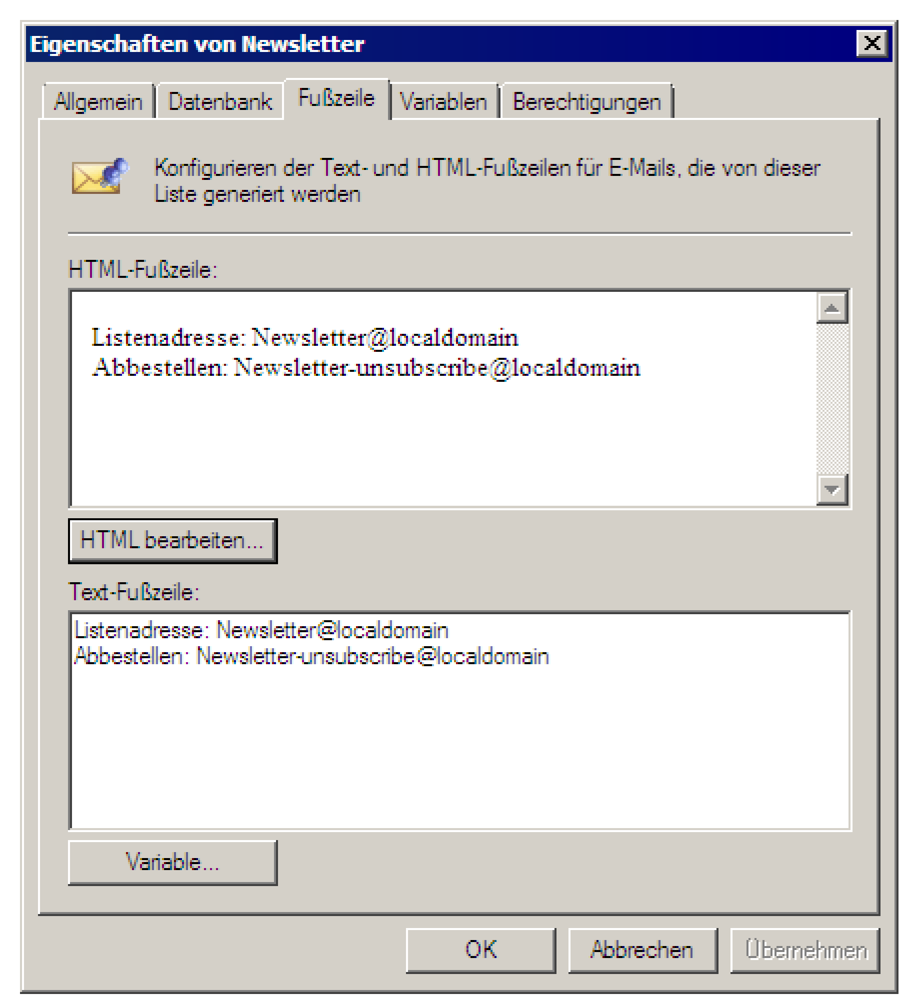


Bild 67 - Newsletter-Fußzeile - Eigenschaften

1. Klicken Sie mit der rechten Maustaste auf die Regel um eine Fußzeile einzufügen und dann auf **Eigenschaften**.

2. Klicken Sie auf der Registerkarte **Fußzeile** auf **HTML bearbeiten** um eine HTML-Fußzeile zu bearbeiten.

HINWEIS: Über die Fußzeile können Sie Benutzern die Möglichkeit einräumen, sich aus der Liste auszutragen und dort einzutragen.

Einstellen von Berechtigungen für die Liste

Geben Sie an, wer E-Mails an die Liste senden darf. Wenn die Liste nicht gesichert ist, kann jeder eine E-Mail an die komplette Liste senden, indem er eine E-Mail an die Listenadresse schickt.

HINWEIS: Berechtigungen für Diskussionslisten lassen sich nicht konfigurieren.

1. Klicken Sie mit der rechten Maustaste auf die Regel um Berechtigungen zu definieren und klicken Sie dann auf **Eigenschaften**.

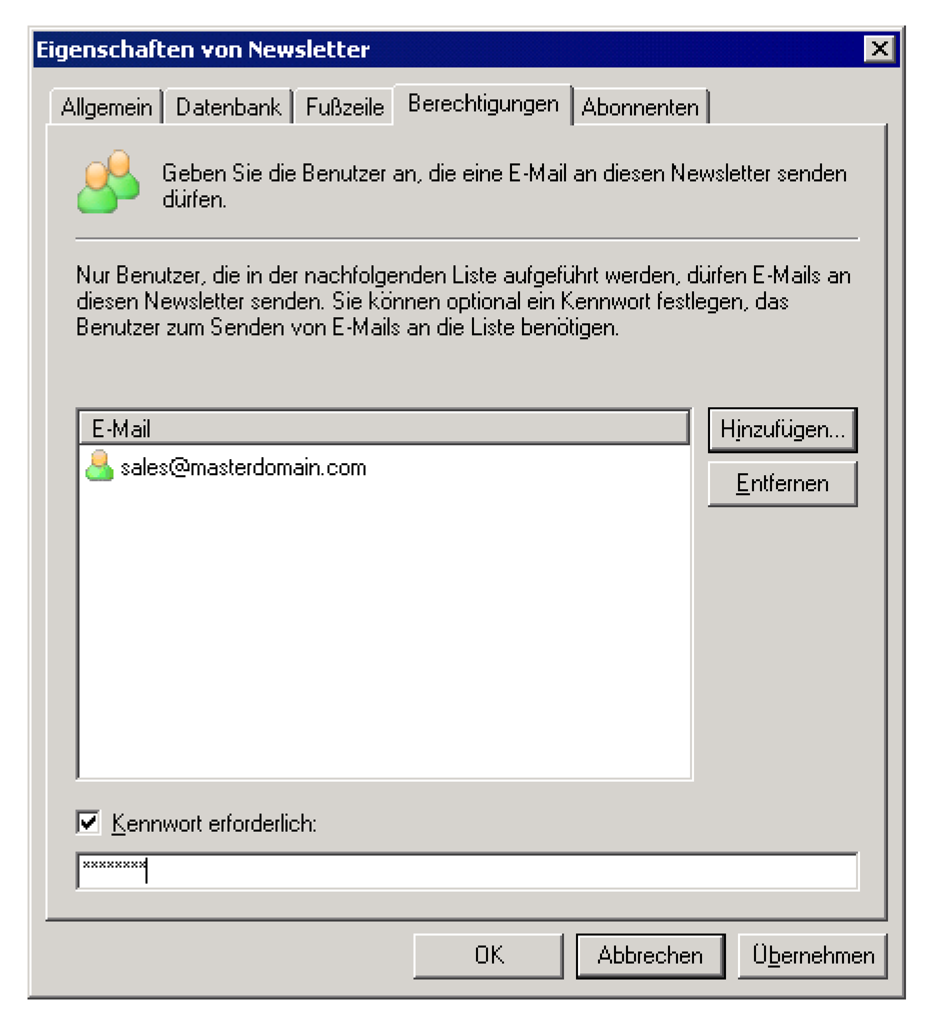


Bild 68 - Einstellen von Berechtigungen für die Liste

2. Klicken Sie auf der Registerkarte **Berechtigungen** auf die Schaltfläche **Hinzufügen** und geben Sie die Benutzer an, die berechtigt sind, eine E-Mail an die Liste zu senden. E-Mail-Adressen werden in der **E-Mail**-Liste hinzugefügt.

3. Aktivieren Sie Kennwörter, indem Sie in das Kontrollkästchen **Kennwort erforderlich** klicken und ein Kennwort angeben. Weitere Informationen, wie Sie diese Funktion nutzen, finden Sie im nächsten Abschnitt: Sichern von Newslettern mit einem Kennwort.

Sichern von Newslettern mit einem Kennwort

Newsletter/Diskussion mit Kennwort sichern - Legen Sie ein Kennwort fest, das den Zugriff auf den Newsletter/die Diskussionsliste sichert, falls jemand den Kontenzugriff eines zulässigen Benutzers oder dessen E-Mail Client verwendet.

HINWEIS: Diskussionslisten können nicht mit Kennwörtern geschützt werden.

1. Klicken Sie mit der rechten Maustaste auf die Regel um Berechtigungen zu definieren und klicken Sie dann auf **Eigenschaften**.

2. Klicken Sie auf der Registerkarte **Berechtigungen** in das Kontrollkästchen **Kennwort erforderlich:** und geben Sie ein Kennwort an.

WICHTIGER HINWEIS: Die Benutzer müssen sich authentifizieren, indem sie das Kennwort in der E-Mail-Betreffzeile eingeben, wenn sie E-Mails an den Newsletter senden. Dieses Kennwort muss im Betreff-Feld wie folgt angegeben werden:

[KENNWORT:<*Kennwort:*>**]** <*Betreff der E-Mail!*>

- **Beispiel:** [KENNWORT:letmepost]Sonderangebot.

Ist das Kennwort richtig, entfernt der Listenserver die Kennwortdaten aus der Betreffzeile und leitet die E-Mail an den Newsletter weiter.

Hinzufügen von Abonnenten zur Liste

Ergänzen Sie Benutzer für Newsletter und Diskussionslisten, ohne dass diese etwas tun müssen.

HINWEIS: Die Benutzer müssen sich bei der Liste anmelden, indem sie eine E-Mail an die Anmeldeadresse für den Newsletter/die Diskussionsliste senden. Werden Benutzer ohne ihre ausdrückliche Zustimmung in Listen hinzugefügt, müssen Sie mit Beschwerden wegen Spam rechnen.

1. Klicken Sie mit der rechten Maustaste auf die Regel um Berechtigungen zu definieren und klicken Sie dann auf **Eigenschaften**.

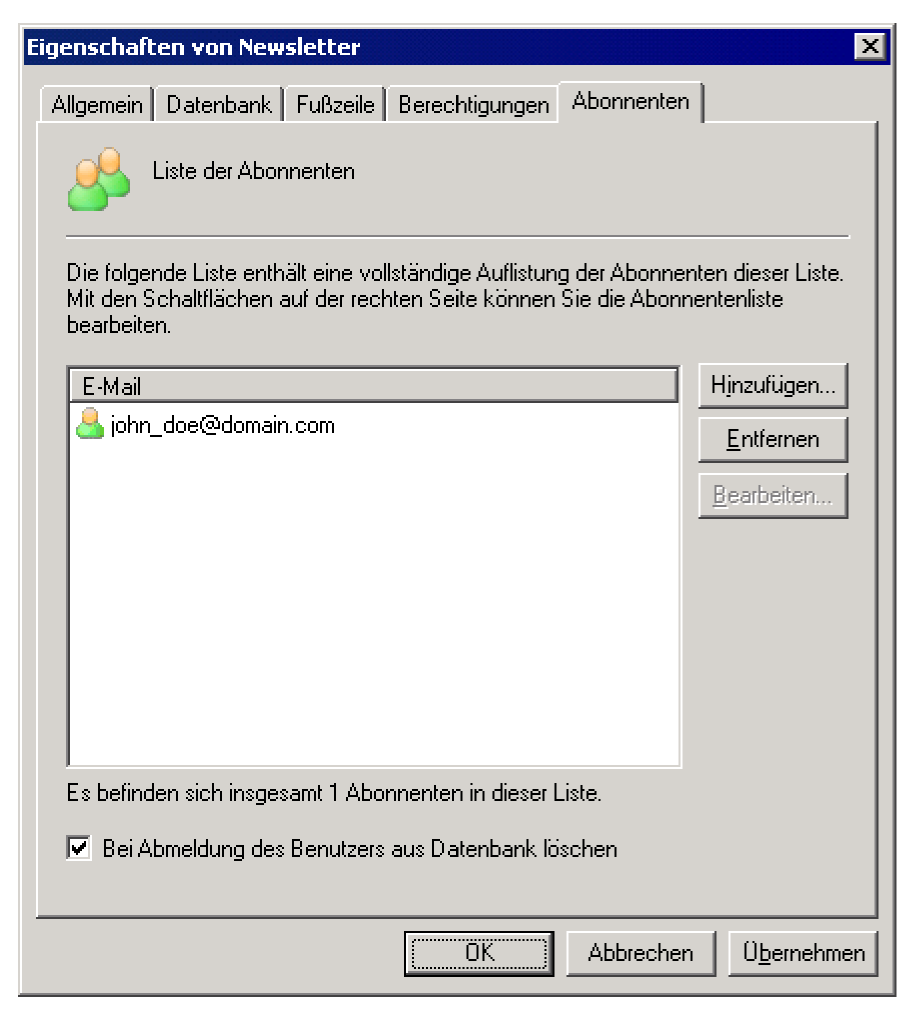


Bild 69 - Eingabe von Teilnehmern für den Newsletter

2. Klicken Sie auf der Registerkarte **Abonnenten** auf die Schaltfläche **Hinzufügen**.

3. Füllen Sie die Felder **E-Mail-Adresse**, **Vorname** und **Nachname** sowie **Firmendaten** aus und klicken Sie auf die Schaltfläche **OK**. Die neue Abonnenten-E-Mail-Adresse wird in der **E-Mail**-Liste hinzugefügt.

HINWEIS 1: Die Felder Vorname, Nachname und Firma sind optional.

HINWEIS 2: Wählen Sie den Benutzer aus und klicken Sie auf die Schaltfläche **Entfernen** um Abonnenten aus der Liste zu entfernen.

HINWEIS 3: Wenn Sie Benutzer aus der Abonnentenlistentabelle entfernen wollen, wenn diese sich von der Liste abmelden (und diese nicht nur als ausgetragen markieren) wollen, klicken Sie in das Kontrollkästchen **Bei Abmeldung des Benutzers aus Datenbank löschen.**

6.3.3 Einsatz von Newslettern/Diskussionslisten

Nach Anlage eines Newsletters/einer Diskussionsliste müssen die Benutzer sich anmelden, damit sie diese erhalten. Folgende Schritte können Benutzer für Newsletter/Diskussionslisten ausführen:

» Einen Newsletter lesen

- Sich bei einer Liste anmelden
- Die Anmeldung abschließen
- Einen Newsletter erstellen
- Sich aus der Liste austragen

Einsatz von Newslettern

- **Anmeldung bei der Liste** - Bitten Sie die Benutzer, eine E-Mail an <newslettername>-subscribe@yourdomain.com zu senden.
- **Abschluss der Eintragung** - Sobald diese Bitte empfangen wird, sendet der Listen-Server eine Bestätigungs-E-Mail zurück. Die Benutzer müssen ihre Eintragung über die Antwort-E-Mail bestätigen, damit sie als Abonnent ergänzt werden.

  HINWEIS: Die Bestätigungs-E-Mail ist obligatorisch und kann nicht abgeschaltet werden.
- **Versenden eines Newsletters/Diskussionslistenbeitrags -** Mitglieder, die die Berechtigung haben, E-Mails an die Liste zu senden, müssen die E-Mail an die E-Mail-Adresse des Newsletters senden: <newslettername>@yourdomain.com
- **Austragung aus der Liste** - Um sich aus der Liste auszutragen, müssen die Benutzer eine E-Mail an folgende E-Mail-Adresse senden: <newslettername>-unsubscribe@yourdomain.com

Tipp: Damit sich Benutzer einfach bei Newslettern anmelden können, sollten Sie ein Webformular mit Feldern für Name und E-Mail-Adresse und direkter Ausgabe an folgende Adresse ergänzen: <newslettername>-subscribe@yourdomain.com

6.3.4 Importieren von Abonnenten in die Liste/Datenbankstruktur

Wenn Sie einen neuen Newsletter oder eine neue Diskussionsliste erstellen, wird bei der Konfiguration eine Tabelle 'Listenname_Abonnenten' mit den unten angezeigten Feldern erstellt.

Um Daten in die Liste zu importieren, müssen Sie die Datenbank mit den richtigen Daten in den richtigen Feldern füllen.

FELDNAME	TYP	STANDARD WERT	KENNZEICHEN	BESCHREIBUNG
Ls_id	Varchar(100)		PK	Abonnent-ID
Ls_first	Varchar(250)			Vorname
Ls_last	Varchar(250)			Nachname
Ls_email	Varchar(250)			E-Mail
Ls_unsubscribed	Int	0	NOT NULL	Austragungske-nnzeichnung
ls_company	Varchar(250)			Name der Firma

6.4 E-Mail-Überwachung

E-Mail-Überwachung erlaubt den Versand von Kopien der von/an bestimmte lokale E-Mail-Adressen gesendeten E-Mails an eine andere E-Mail-Adresse. Auf diese Weise können Sie zentrale Speicher der E-Mail-Kommunikation für bestimmte Personen oder Abteilungen anlegen.

Sie können diese Funktion auch als Ersatz für eine E-Mail-Archivierung benutzen, da die E-Mails automatisch an Microsoft Exchange Server oder Microsoft Outlook gesendet werden.

6.4.1 Aktivieren/Deaktivieren der E-Mail-Überwachung

1. Klicken Sie mit der rechten Maustaste auf **E-Mail-Verwaltung ► E-Mail-Überwachung** und dann auf **Eigenschaften.**

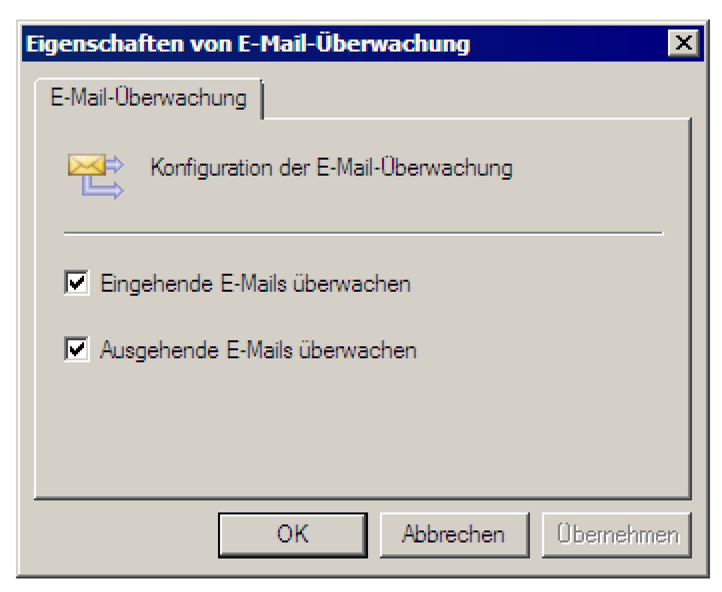


Bild 70 - E-Mail-Überwachung aktivieren oder deaktivieren

2. Aktivieren/deaktivieren Sie alle Überwachungsregeln für eingehende und ausgehende E-Mails, indem Sie die Kontrollkästchen **Eingehende Überwachung aktivieren** und **Ausgehende Überwachung aktivieren** deaktivieren oder aktivieren.

3. Klicken Sie auf **OK** um die Änderungen zu speichern.

HINWEIS: Aktivieren/deaktivieren Sie die Regeln zur Überwachung einzelner E-Mails, indem Sie mit der rechten Maustaste auf die Regeln zur E-Mail-Überwachung klicken, und dann die Option **Aktivieren/Deaktivieren** auswählen.

6.4.2 E-Mail-Überwachung konfigurieren

1. Klicken Sie mit der rechten Maustaste auf **E-Mail-Verwaltung ► E-Mail-Überwachung** und dann auf **Neu ► Überwachungsregel für eingehende Post oder** E-Mail-Überwachungsregel für ausgehende Post um eingehende oder ausgehende Post entsprechend zu überwachen.

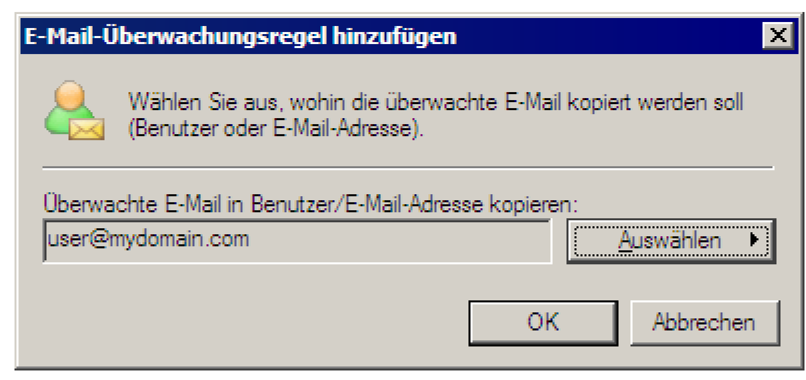


Bild 71 - E-Mail-Überwachungsregel hinzufügen

2. Geben Sie die Ziel-E-Mail-Adresse/das Zielpostfach an, in das E-Mails kopiert werden sollen. Klicken Sie auf **OK** um fortzufahren.

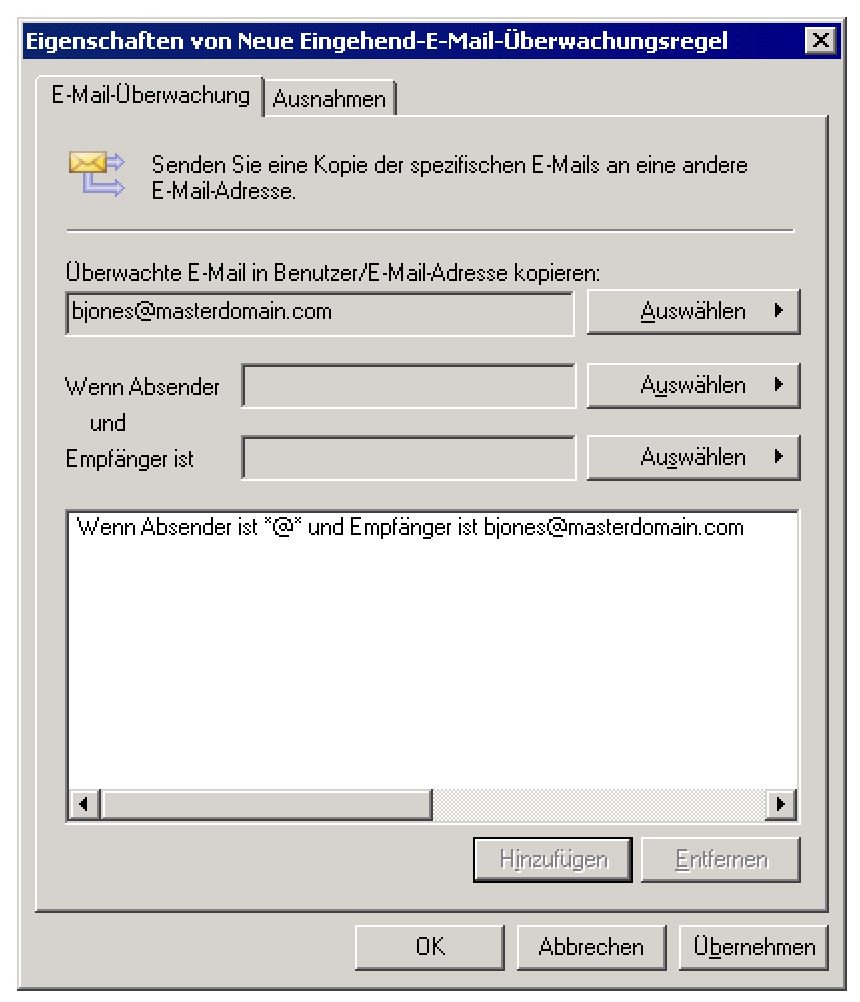


Bild 72 - Konfiguration der E-Mail-Überwachung

3. Klicken Sie auf Absender und Empfänger. **Wählen Sie mit den** Schaltflächen aus, welche E-Mails mit dieser Regel überwacht werden sollen. Klicken Sie auf **Hinzufügen** um Filter in der Liste hinzuzufügen. Wiederholen Sie die Schritte um mehrere Filter zu definieren. Die folgenden Bedingungen können überwacht werden:

HINWEIS: Wenn Sie alle E-Mails überwachen wollen, geben Sie *@* ein.

- **Alle von einem bestimmten Benutzer versendeten E-Mails** - Erstellen Sie eine Regel für ausgehende E-Mails, geben Sie die E-Mail des Absenders an oder wählen Sie den Benutzer (wenn Sie Active Directory verwenden) im Absenderfeld aus und geben Sie *@* als Domäne des Empfängers an.
- **Alle E-Mails, die an einen bestimmten Benutzer versendet werden**- Erstellen Sie eine Regel für eingehende E-Mails, definieren Sie in dem Empfängerfeld die E-Mails des Empfängers oder wählen Sie den Benutzer (wenn Sie Active Directory verwenden) aus und geben Sie *@* als Domäne des Absenders an.
- **Von einem bestimmten Benutzer gesendete E-Mail an einen externen Empfänger -** Erstellen Sie eine Regel für ausgehende E-Mails und geben Sie den Absender an oder wählen Sie den Benutzer bei Verwendung von Active Directory im Feld "Absender" aus. Geben Sie die E-Mail des externen Empfängers im Empfängerfeld ein.
- **Von einem externen Absender an einen bestimmten Benutzer gesendete E-Mail -** Erstellen Sie eine Regel für eingehende E-Mail und geben Sie in dem Feld "Absender" die E-Mail-Adresse des externen Absenders an. Geben Sie im Feld "Empfänger" den Benutzernamen oder die E-Mail-Adresse des Benutzers ein.
- **Von einem bestimmten Benutzer an eine Firma oder Domäne gesendete E-Mail -** Erstellen Sie eine Regel für ausgehende E-Mail und geben Sie den Absender bzw. den Benutzer (bei Verwendung von Active Directory) in dem Feld "Absender" ein. Geben Sie die

Domäne der Firma in dem Feld "Empfänger" ein, indem Sie die **Domäne** über die Schaltfläche **Empfänger** auswählen.

- **Von einer Firma oder Domäne an bestimmte Benutzer gesendete E-Mail -** Erstellen Sie eine Regel für eingehende E-Mail und geben Sie die Domäne der Firma im Feld "Absender" ein. Wählen Sie die **Domäne** durch Klicken auf die Schaltfläche **Absender** aus und geben Sie den Benutzernamen bzw. die E-Mail-Adresse des Benutzers im Feld "Empfänger" ein.

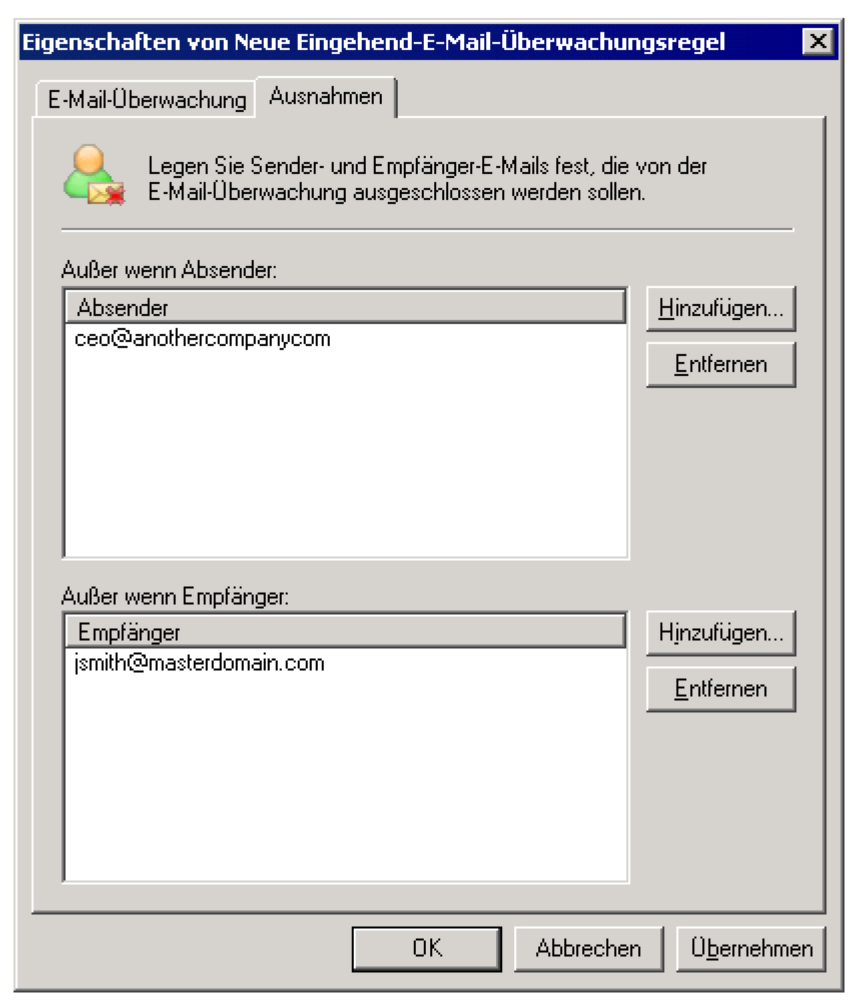


Bild 73 - Erstellen einer Ausnahme

4. Klicken Sie auf die Registerkarte Ausnahmen um Absender oder Empfänger hinzuzufügen, die bei der neuen Regel nicht berücksichtigt werden sollen. Die verfügbaren Optionen sind:

- **Außer wenn Absender gleich** - Schließt den angegebenen Absender aus der Liste aus.
- **Außer wenn Empfänger gleich** - Schließt den angegebenen Empfänger aus der Liste aus.

HINWEIS 1: Bei der Definition von Ausnahmen für Überwachungsregeln eingehender E-Mails enthält die **Absenderliste** nicht-lokale E-Mail-Adressen und die **Empfängerliste** nur lokale E-Mail-Adressen. Bei der Definition von Ausnahmen für eine Überwachungsregel ausgehender E-Mails enthält die **Absenderliste** lokale E-Mail-Adressen und die **Empfängerliste** nur nicht-lokale E-Mail-Adressen.

HINWEIS 2: Es werden beide Ausnahmelisten berücksichtigt und die in der Absender-Ausnahmeliste enthaltenen Absender sowie alle in der Empfänger-Ausnahmeliste enthaltenen Empfänger werden nicht überwacht.

5. Klicken Sie auf **OK** um die Einstellungen zu übernehmen.

HINWEIS: Eine neue E-Mail-Überwachungsregel können Sie umbenennen, indem Sie auf die E-Mail-Überwachungsregel klicken und dann die Taste F2 drücken.

7 Anpassen des Setups von GFI MailEssentials

7.1 Lokale Domänen

Anhand der Domänen eingehender E-Mails kann GFI MailEssentials zwischen eingehenden und ausgehenden E-Mails unterscheiden und somit die E-Mails identifizieren, die auf Spam untersucht werden sollten. Bei der Installation werden die Domänen der eingehenden E-Mails über den Dienst IIS SMTP importiert.

In einigen Fällen kann jedoch eine lokale E-Mail-Umleitung in IIS eine abweichende Konfiguration erfordern:

Beispiel: Dies trifft zu für Domänen, die für E-Mail-Umleitung lokal sind, für Ihren Mail-Server jedoch nicht.

Die Anweisungen in diesem Abschnitt erläutern, wie Sie nach der Installation Domänen eingehender E-Mails ergänzen oder entfernen.

Wichtige Hinweise

1. Jede Domäne, über die Sie E-Mails empfangen und die nicht in der Konfiguration für Domänen eingehender E-Mails aufgeführt ist, ist nicht durch GFI MailEssentials vor Spam geschützt.

7.1.1 Hinzufügen und Entfernen von Inbound-Domänen

1. Klicken Sie mit der rechten Maustaste auf den Knoten **Allgemein ► Allgemein Einstellungen**, dann auf **Eigenschaften** und auf die Registerkarte **Lokale Domänen**.

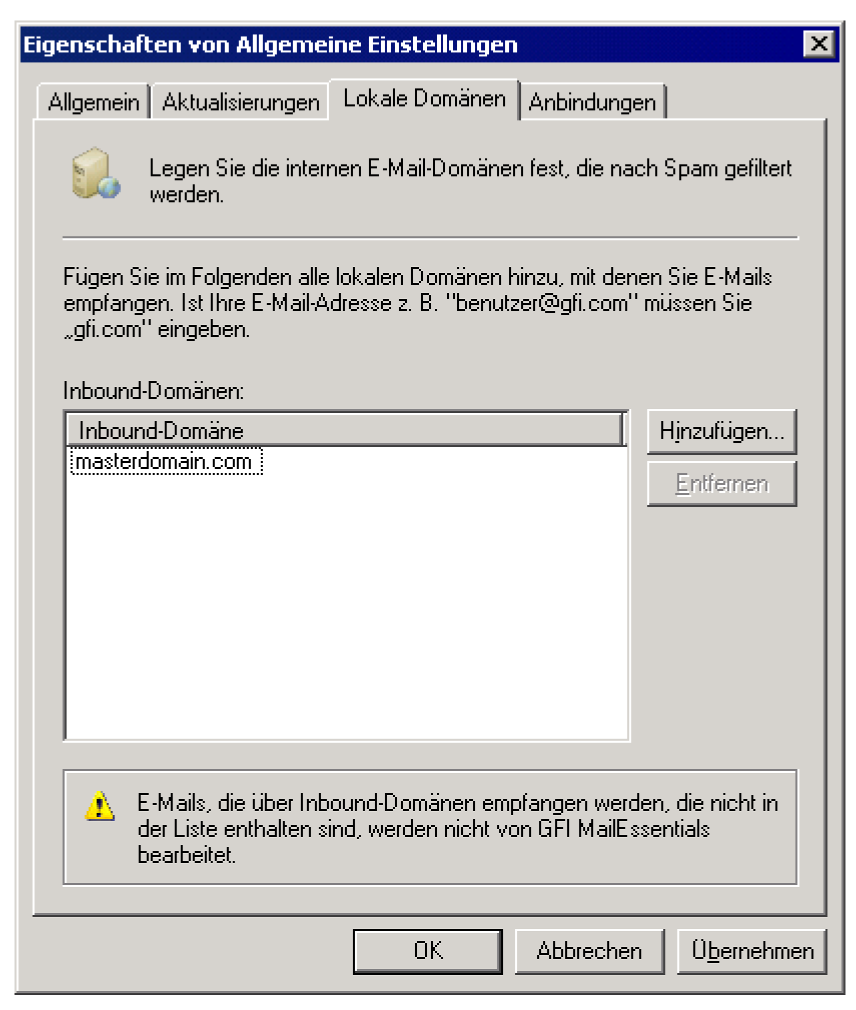


Bild 74 - Hinzufügen einer Domäne für eingehende E-Mails

2. Klicken Sie auf die Schaltfläche **Hinzufügen...** und geben Sie die Details der Domäne ein, die Sie als neue Domäne für eingehende E-Mails hinzufügen wollen. Wählen Sie zum Entfernen von Domänen die betreffende Domäne aus und klicken Sie auf **Entfernen**.

3. Klicken Sie auf **OK** um die Einstellungen zu übernehmen.

7.2 Administrator-E-Mail-Adresse

GFI MailEssentials schickt verschiedene E-Mail-Benachrichtigungen an den Administrator. Diese beinhalten Warnungen, Spam-Übersichten und Update-Benachrichtigungen.

So konfigurieren Sie die E-Mail-Adresse des Administrators:

1. Klicken Sie in der GFI MailEssentials-Konfiguration mit der rechten Maustaste auf **GFI MailEssentials ► Allgemein ► Allgemeine Einstellungen**, und wählen Sie **Eigenschaften**.

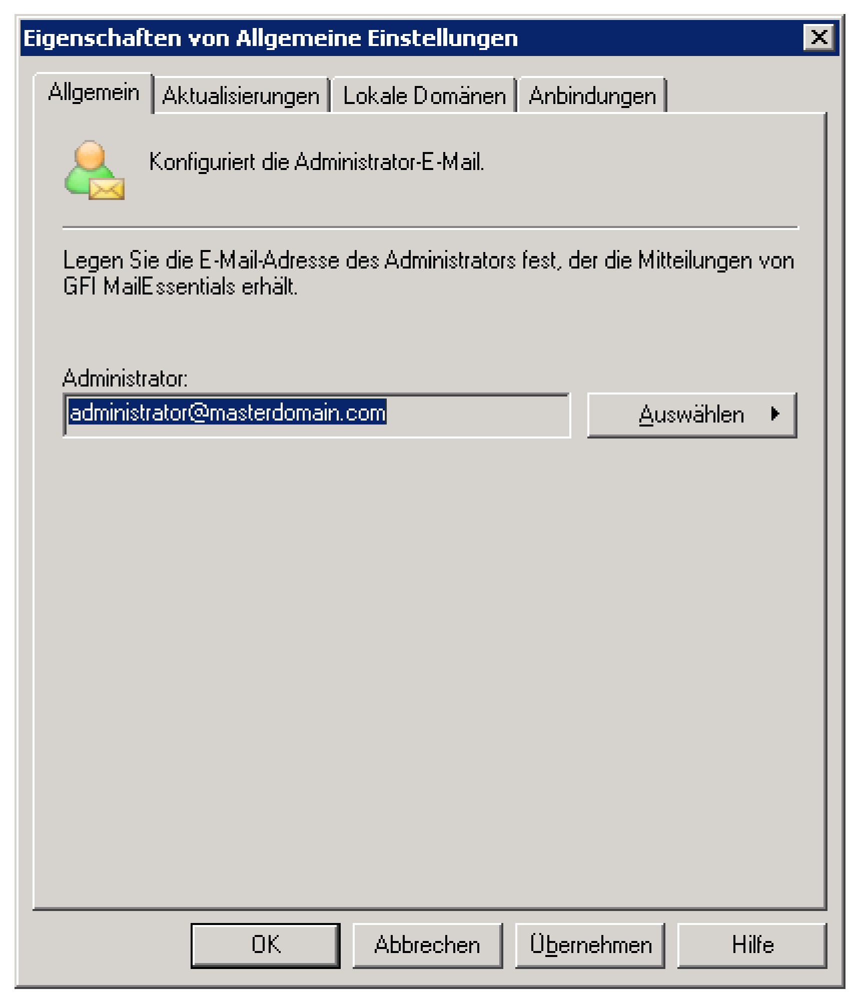


Bild 75 - Administrator-E-Mail-Adresse

2. Klicken Sie auf der Registerkarte „Allgemein“ auf **Auswählen**, und legen Sie einen Benutzer oder eine E-Mail-Adresse fest.

3. Klicken Sie auf **OK**, um die Einstellungen abzuschließen.

7.3 DNS-Servereinstellungen

DNS-Servereinstellungen sind in GFI MailEssentials sehr wichtig, da die IP-DNS-Blocklist und URI-DNS-Blocklist bei der Spam-Filterung eine Domänensuche durchführen. Andere Anti-Spam-Filter verwenden auch DNS, um Spam zu filtern (z. B. SpamRazer).

So legen Sie einen DNS-Server fest:

1. Klicken Sie in der GFI MailEssentials-Konfiguration mit der rechten Maustaste auf **GFI MailEssentials ► Anti-Spam ► Anti-Spam-Einstellungen**, und wählen Sie **Eigenschaften**.

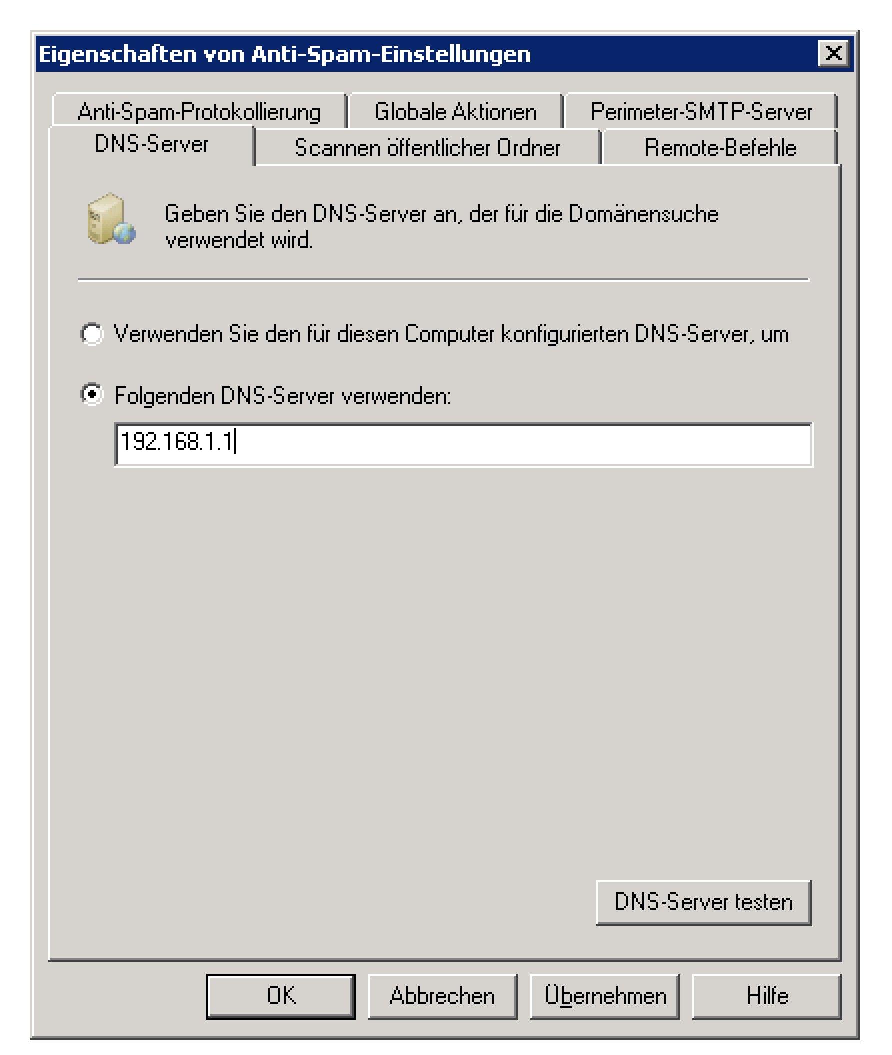


Bild 76 - DNS-Servereinstellungen

2. Wählen Sie auf der Registerkarte „DNS-Server" Folgendes aus:

- **Verwenden Sie den für diesen Computer konfigurierten DNS-Server** - Wählen Sie diese Option, um den gleichen DNS-Server wie das Betriebssystem zu verwenden, unter dem GFI MailEssentials installiert ist.
- **Folgenden DNS-Server verwenden** - Wählen Sie diese Option, um einen DNS-Server festzulegen, der sich vom Server des lokalen Rechners unterscheidet.

3. Klicken Sie auf **DNS-Server testen**, um die Verbindung mit dem festgelegten DNS-Server zu testen. Falls der Test nicht erfolgreich ist, wählen Sie einen anderen DNS-Server.

4. Klicken Sie auf **OK**, um die Einstellungen abzuschließen.

7.4 SMTP-Servereinstellungen

SMTP-Server, die E-Mails an den GFI MailEssentials-Server umleiten, müssen für verschiedene Anti-Spam-Filtermodule wie IP-DNS-Blocklist und Greylist festgelegt sein.

So legen Sie Perimeter-SMTP-Server fest:

1. Klicken Sie in der GFI MailEssentials-Konfiguration mit der rechten Maustaste auf **GFI MailEssentials ► Anti-Spam ► Anti-Spam-Einstellungen**, und wählen Sie **Eigenschaften**.

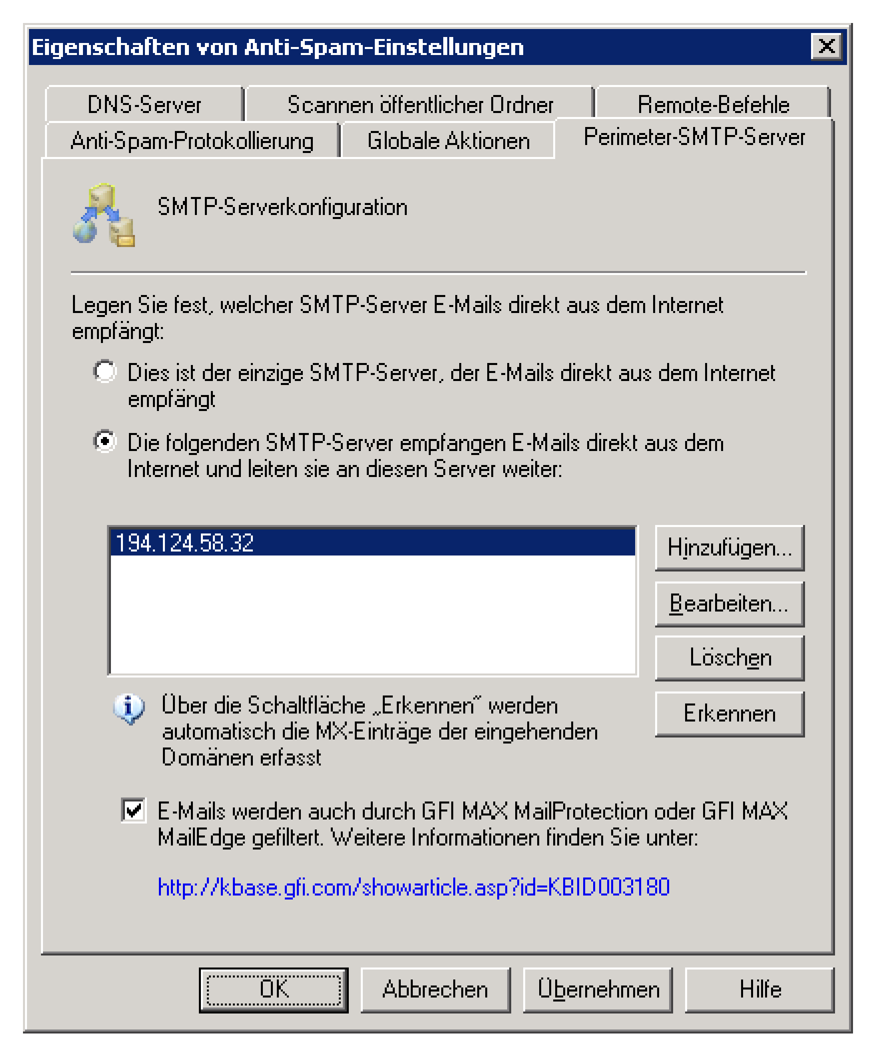


Bild 77 - Perimeter-SMTP-Servereinstellungen

2. Wählen Sie auf der Registerkarte „Perimeter-SMTP-Server" Folgendes aus:

- **Dies ist der einzige SMTP-Server, der E-Mails direkt aus dem Internet empfängt**, wenn GFI MailEssentials nur auf dem SMTP-Server installiert ist, der externe E-Mails direkt aus dem Internet empfängt.
- **Die folgenden SMTP-Server empfangen E-Mails direkt aus dem Internet und leiten sie an diesen Server weiter**, wenn E-Mails von anderen SMTP-Servern an den GFI MailEssentials-Server weitergeleitet werden. Klicken Sie auf **Erkennen**, damit GFI MailEssentials automatisch SMTP-Server erkennt, indem die MX-Einträge der eingehenden Domänen abgefragt werden. Klicken Sie auf **Hinzufügen**, um die IP-Adressen von anderen SMTP-Servern manuell hinzuzufügen, die E-Mails an den GFI MailEssentials-Server umleiten und nicht automatisch hinzugefügt wurden.

  HINWEIS: Beim manuellen Hinzufügen von IP-Adressen von Perimeter-SMTP-Servern können Sie auch einen IP-Adressbereich in CIDR-Notation hinzufügen.
- **E-Mails werden auch durch GFI MAX MailProtection oder GFI MAX MailEdge gefiltert**, wenn die gehosteten E-Mail-Sicherheitsprodukte GFI MAX MailProtection oder GFI MAX MailEdge verwendet werden. Weitere Informationen finden Sie unter:

  http://kbase.gfi.com/showarticle.asp?id=KBID003180

3. Klicken Sie auf **OK**, um die Konfiguration abzuschließen.

7.5 Automatischer Updates

GFI MailEssentials kann so konfiguriert werden, dass automatisch nach Updates gesucht und diese heruntergeladen werden.

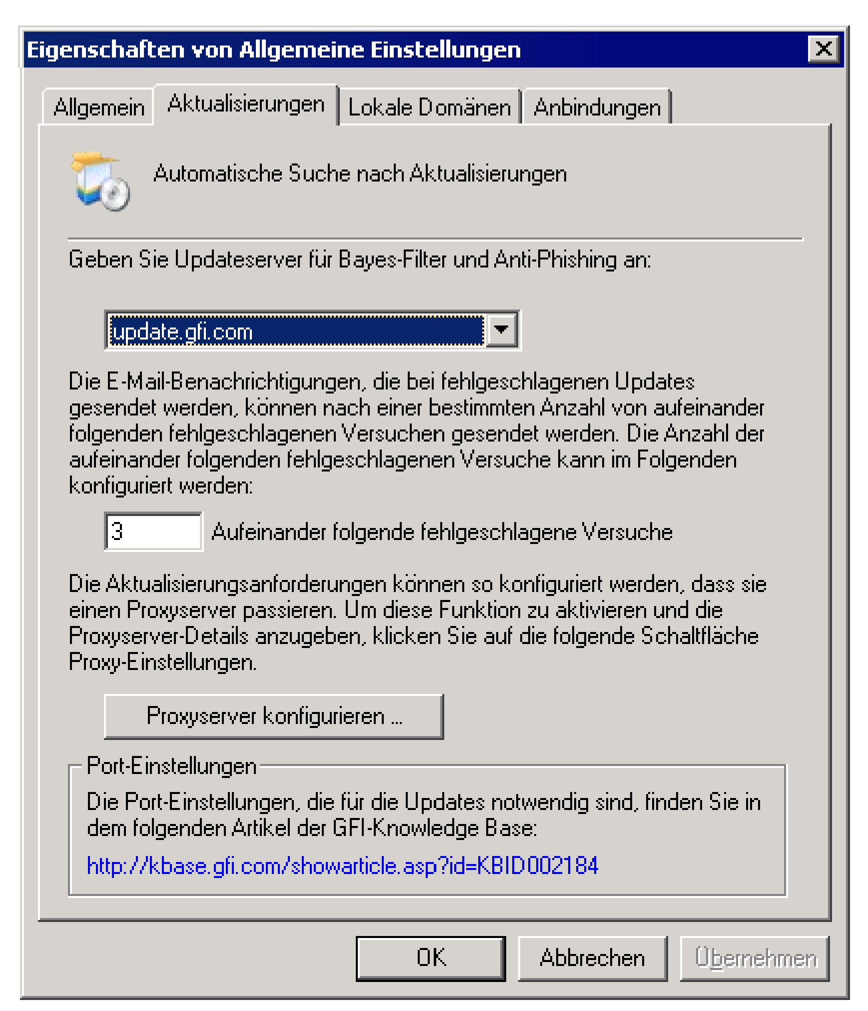


Bild 78 - Konfigurieren automatischer Updates

1. Klicken Sie zur Konfiguration automatischer Updates auf den Knoten **Allgemein ► Allgemeine Einstellungen**, klicken Sie dann auf die Registerkarte **Eigenschaften** und dann auf **Aktualisierungen**.

   - Geben Sie an, auf welchen Servern nach Updates gesucht werden soll, und laden Sie Bayes-Spamfilter-Updates und Anti-Phishing-Updates herunter.
   - Geben Sie an, wie oft ein Update hintereinander fehlschlagen darf, bevor eine E-Mail-Nachricht gesendet wird.
   - Um Updates über einen Proxyserver herunterzuladen, klicken Sie auf **Proxyserver konfigurieren …** . Geben Sie in dem Dialog "Proxy-Einstellungen" die Einstellungen für den Proxyserver an.

2. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

8 Verschiedenes

In diesem Abschnitt werden alle anderen Funktionen beschrieben, die nicht zur Erstkonfiguration, zur Routineverwaltung und zur kundenspezifischen Anpassung von GFI MailEssentials gehören.

8.1 Konfiguration von POP3 und Download-Einwahlverbindung

Das Post Office Protocol (POP3 nach RFC 1225) ist ein Client Server-Protokoll zur Speicherung von E-Mails, damit Clients eine Verbindung mit dem POP3-Server jederzeit aufbauen und die E-Mails lesen können. Ein Mail Client stellt die TCP/IP-Verbindung mit dem Server her, sodass die Benutzer nach Austausch verschiedener Befehle die E-Mail lesen können. Alle ISPs unterstützen POP3.

Wir empfehlen für GFI MailEssentials, POP3 möglichst nicht zu verwenden, sondern SMTP, da POP3 für E-Mail Clients konzipiert ist und nicht für Mail-Server. Trotzdem kann es Situationen geben, in denen eine statische IP-Adresse für SMPT nicht verfügbar ist, daher kann GFI MailEssentials E-Mails über POP3 abholen.

8.1.1 Konfiguration des POP3-Downloaders

1. Klicken Sie auf den Knoten **POP2Exchange** und doppelklicken Sie auf den Eintrag **Allgemein**.

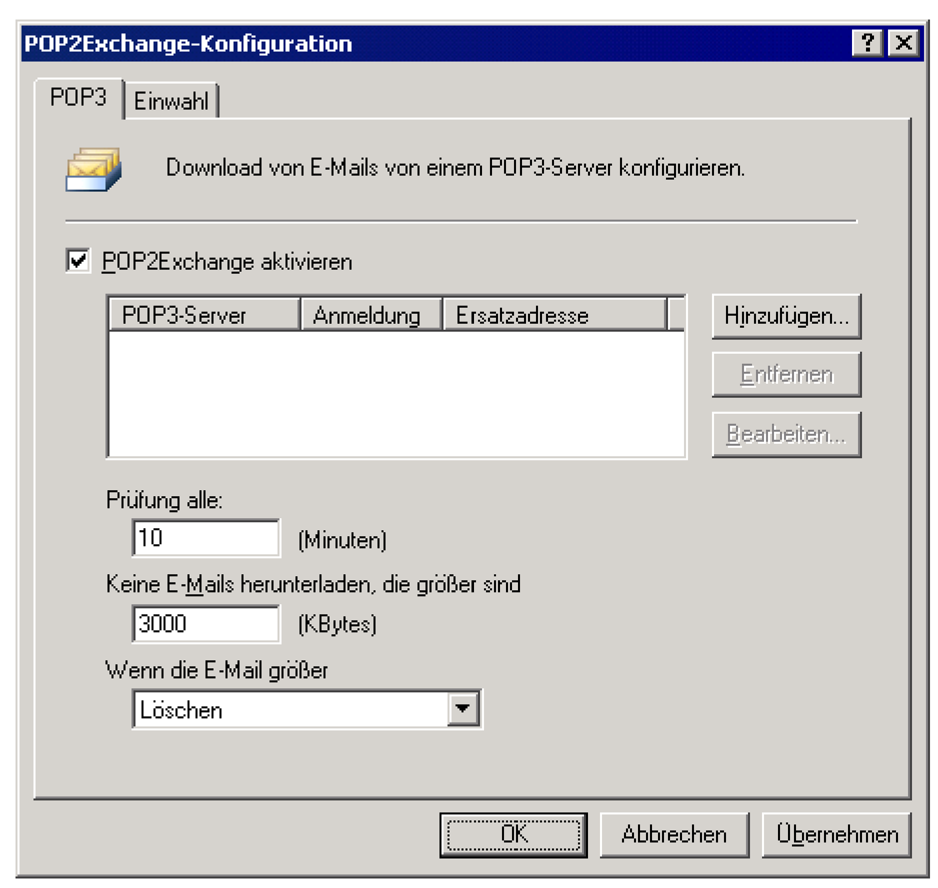


Bild 79 - POP3-Downloader von GFI MailEssentials

2. Klicken Sie auf der Registerkarte **POP3** in das Kontrollkästchen **POP2Exchange** aktivieren um den POP3-Downloader zu aktivieren.

3. Klicken Sie auf **Hinzufügen** um eine POP3-Mail-Box hinzuzufügen, in die E-Mails heruntergeladen werden.

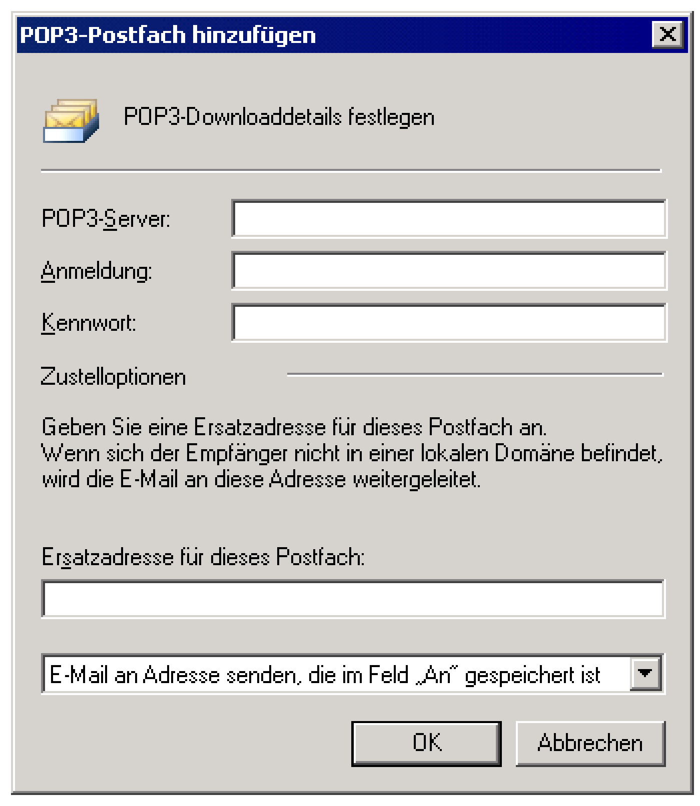


Bild 80 - Hinzufügen eines POP3- Postfachs

4. Geben Sie die POP3-Serverdetails, den Benutzernamen und das Kennwort für das Postfach ein. Wählen Sie zwischen folgenden Optionen:

- **Mail an die in dem Feld 'To' gespeicherte E-Mail-Adresse senden -** GFI MailEssentials analysiert den E-Mail-Header und leitet die E-Mail entsprechend um. Wenn die E-Mail-Analyse fehlschlägt, wird die E-Mail an eine in dem Feld Ersatzadresse angegebene E-Mail-Adresse gesendet.
- **Mail an Ersatzadresse senden:** Alle E-Mails aus diesem Postfach werden an eine E-Mail-Adresse weitergeleitet. Geben Sie die vollständige SMTP-Adresse in dem Feld 'E-Mail-Adresse' ein.
    - **Beispiel:** john@company.com

5. Geben Sie die Ersatzadresse ein und klicken Sie auf **OK**.

HINWEIS 1: Wenn Sie die Zieladresse angeben (die Adresse, an die GFI MailEssentials die E-Mail weiterleitet), müssen Sie kontrollieren, ob Sie die betreffende SMTP-Adresse auf Ihrem Mailserver konfiguriert haben.

HINWEIS 2: Es können mehrere POP3 -Postfächer konfiguriert werden.

6. Konfigurieren Sie in dem Konfigurationsdialog POP2Exchange die anderen verfügbaren Optionen:

- **In folgendem Intervall prüfen (Minuten):** Definieren Sie das Intervall zum Herunterladen.
- **Keine E-Mail herunterladen, die größer ist als (Kilobyte):** Geben Sie die maximale Datengröße für das Herunterladen an. Wenn die E-Mail größer ist, wird sie nicht heruntergeladen.
- **Bei größerer E-Mail wie folgt verfahren:** Löschen Sie E-Mails, die größer sind als maximal zulässig, oder senden Sie eine Nachricht an den Postmaster.

8.1.2 Einwahl-Verbindungsoptionen konfigurieren

1. Klicken Sie auf den Knoten **POP2 Exchange** und doppelklicken Sie auf den Eintrag **Allgemein**.

2. Klicken Sie auf der Registerkarte **Einwahl** in das Kontrollkästchen **E-Mails per automatischer Einwahl oder bei Bedarf empfangen** um die Einwahlverbindung zu aktivieren.

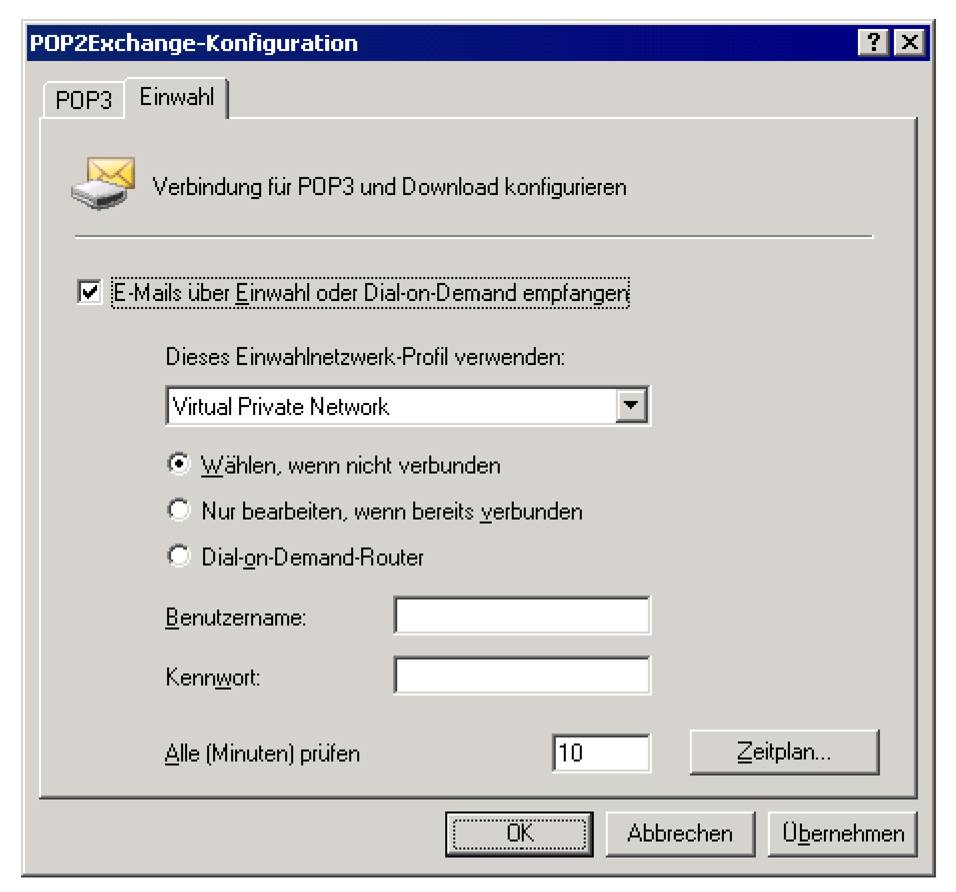


Bild 81 - Einwahloptionen

3. Wählen Sie ein Einwahlnetzwerkprofil aus und konfigurieren Sie einen Benutzernamen und ein Kennwort. Folgende Optionen sind verfügbar:

- **Dieses Einwahlnetzwerkprofil verwenden:** Wählen Sie, welches Einwahlnetzwerkprofil verwendet werden soll.
- **Einwahl, wenn keine Verbindung vorhanden:** GFI MailEssentials benutzt die Einwahlverbindung nur dann, wenn keine Verbindung existiert.
- **Benutzername:** Geben Sie den verwendeten Benutzernamen für die Anmeldung bei ISP ein.
- **Kennwort:** Geben Sie das Kennwort für die Anmeldung bei Ihrem ISP ein.
- **Nur verarbeiten, wenn Verbindung vorhanden:** GFI MailEssentials verarbeitet E-Mails nur dann, wenn bereits eine Verbindung existiert.
- **Bei Bedarf über Router einwählen:** Falls eine Internetverbindung vorhanden ist, die automatisch hergestellt wird (beispielsweise nach Bedarf bei Einwahl über einen Router), wählen Sie diese Option aus. GFI MailEssentials holt die E-Mails in den definierten Zeitabständen ab, ohne selbst eine Einwahlverbindung aufzubauen.
- **Alle (Minuten) bearbeiten):** Geben Sie ein, wie oft GFI MailEssentials eine Einwahlverbindung herstellen oder prüfen soll, ob bereits eine Verbindung existiert (je nachdem, ob Sie GFI MailEssentials für eine Einwahlverbindung konfigurieren oder E-Mails nur verarbeitet werden sollen, wenn bereits eine Verbindung existiert).

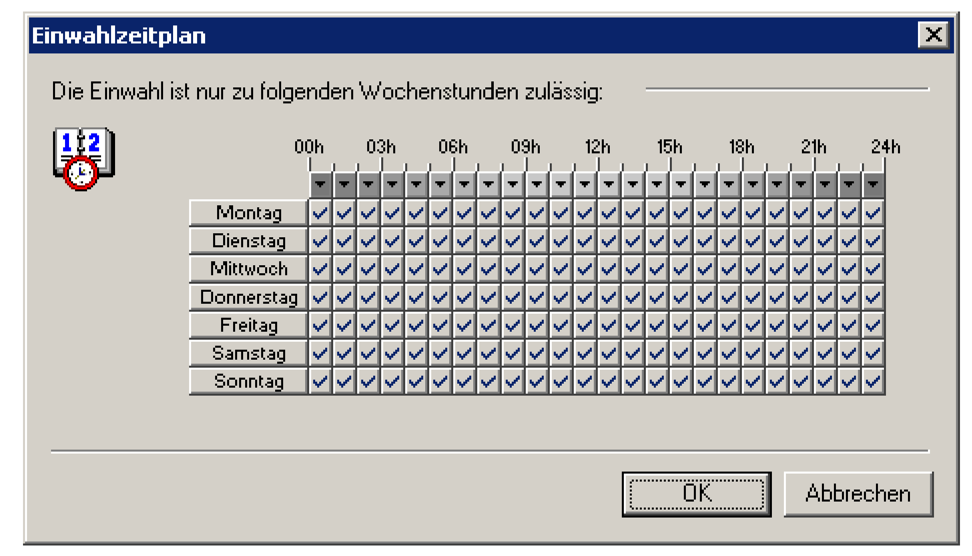


Bild 82 - Konfiguration der E-Mail-Abholung durch GFI MailEssentials

4. Klicken Sie auf **Zeitplan** und geben Sie an, zu welcher Uhrzeit GFI MailEssentials eine Einwahlverbindung herstellen und E-Mails abholen soll. Ein Häkchen gibt an, dass GFI MailEssentials eine Einwahlverbindung herstellt. Ein Kreuz gibt an, dass GFI MailEssentials in dieser Stunde keine Einwahlverbindung herstellt.

5. Klicken Sie auf **OK** um die Konfiguration zu übernehmen.

8.2 Synchronisieren der Konfigurationsdaten

Wenn GFI MailEssentials auf mehreren Servern installiert ist, müssen die Anti-Spam- und Konfigurationsdaten zwischen den Servern synchronisiert werden.

GFI MailEssentials automatisiert diesen Vorgang durch zwei Funktionen, mit denen sich mehrere Installationen von GFI MailEssentials synchronisieren lassen:

- Konfiguration des Anti-Spam Synchronization Agent: Dieser Dienst synchronisiert die Anti-Spam-Einstellungen verschiedener Installationen von GFI MailEssentials mit dem Microsoft BITS-Dienst.
- Exportieren und Importieren von GFI MailEssentials-Einstellungen: Mit dieser Anwendung können alle Konfigurationseinstellungen von GFI MailEssentials exportiert und importiert werden; die Konfiguration einer neuen Installation von GFI MailEssentials kann mit genau denselben Einstellungen wie bei einer funktionsfähigen Installation von GFI MailEssentials erfolgen.

8.2.1 Anti-Spam Synchronization Agent

Der Anti-Spam Synchronization Agent arbeitet wie folgt:

1. Ein Server, der als Host für GFI MailEssentials dient, ist als Master-Server konfiguriert.

2. Die anderen Server, auf denen GFI MailEssentials installiert ist, sind als Slave-Server konfiguriert.

3. Die Slave-Server laden eine Archivdatei mit den Anti-Spam-Einstellungen in einen virtuellen IIS-Ordner auf dem Master-Server über den BITS-Dienst hoch.

4. Wenn der Master-Server alle Anti-Spam-Daten der Slave-Server erfasst hat, werden die Daten aus den einzelnen Archiven extrahiert und in einer neuen aktuellen Archivdatei für die Anti-Spam-Einstellungen zusammengeführt.

5. Die Slave-Server laden diese aktualisierte Archivdatei mit den Anti-Spam-Einstellungen herunter, extrahieren sie und aktualisieren die lokale Installation von GFI MailEssentials mit den neuen Einstellungen.

HINWEIS 1: Auf allen Servern, deren Anti-Spam-Daten synchronisiert werden sollen, muss die gleiche Version von GFI MailEssentials installiert sein.

HINWEIS 2: Die durch den Anti-Spam Synchronization Agenten hochgeladenen und heruntergeladenen Dateien sind komprimiert um den Traffic im Netzwerk zu begrenzen.

8.2.2 Schritt 1: Konfigurieren des virtuellen Verzeichnisses für den Synchronisations-Agenten auf dem Master-Server

Wichtige Hinweise

1. Es kann immer nur ein Server als Master-Server konfiguriert werden.

2. Ein Server muss folgende Systemspezifikationen erfüllen, wenn er als Master-Server konfiguriert werden soll:

- Microsoft Windows Server 2008 mit SP1 oder höher und IIS7.0 mit installierter BITS-Server-Erweiterung. (Weitere Informationen zur Installation der BITS-Server-Erweiterung finden Sie weiter unten.)
- Microsoft Windows Server 2003 mit SP1 oder höher und IIS6.0 mit installierter BITS-Server-Erweiterung. (Weitere Informationen zur Installation der BITS-Server-Erweiterung finden Sie weiter unten.)

3. Installieren Sie die Microsoft BITS-Servererweiterungen:

- Windows Server 2003 siehe:

  http://technet.microsoft.com/en-us/library/cc740133(WS.10).aspx
- Windows Server 2008 siehe:

  http://technet.microsoft.com/en-us/library/cc753301.aspx

4. Ein virtuelles IIS-Verzeichnis sollte nur auf dem Master-Server erstellt werden.

Konfigurieren des virtuellen Verzeichnisses für den Synchronisations-Agenten

Konfigurieren Sie in Internet Information Services (IIS) Manager wie nachfolgend beschrieben ein gemeinsames virtuelles Verzeichnis auf der Standard-Website des Master-Servers.

IIS 7.0

a. Laden Sie die Konsole **Internet Information Services (IIS) Manager**, klicken Sie mit der rechten Maustaste auf die gewünschte Website, und wählen Sie **Virtuelles Verzeichnis hinzufügen**.

b. Geben Sie im Dialogfeld **Virtuelles Verzeichnis hinzufügen** den Alias **MESynchAgent** für das virtuelle Verzeichnis ein.

c. Legen Sie einen Pfad fest, unter dem der Inhalt des virtuellen Verzeichnisses gespeichert werden soll, und klicken Sie auf **OK**, um das virtuelle Verzeichnis hinzuzufügen.

HINWEIS: Merken Sie sich den konfigurierten Pfad für eine spätere Verwendung.

d. Wählen Sie das virtuelle Verzeichnis **MESynchAgent** aus, und doppelklicken Sie in der Funktionsansicht auf **SSL-Einstellungen**.

e. Deaktivieren Sie das Kontrollkästchen **SSL erfordern**, und klicken Sie auf **Übernehmen**.

f. Kehren Sie zur Funktionsansicht des gerade erstellten virtuellen Verzeichnisses zurück, und doppelklicken Sie auf **Authentifizierung**.

g. Stellen Sie sicher, dass nur **Standardauthentifizierung** aktiviert ist. Alle andere Optionen müssen deaktiviert sein.

h. Klicken Sie mit der rechten Maustaste auf **Standardauthentifizierung**. Klicken Sie anschließend auf **Bearbeiten…**, um die **Standarddomäne** und den **Bereich** für Benutzername und Passwort festzulegen, die von Slave-Rechnern für die Authentifizierung verwendet werden sollen. Klicken Sie auf **OK** und auf **Übernehmen**.

i. Kehren Sie zur Funktionsansicht des virtuellen Verzeichnisses **MESynchAgent** zurück, und doppelklicken Sie auf **BITS-Uploads**.

j. Wählen Sie **Datei-Upload für Clients zulassen** und **Standardeinstellungen von übergeordnetem Ordner verwenden**. Klicken Sie auf **Übernehmen**.

IIS 6.0

a. Laden Sie aus **Verwaltung** die Konsole **Internet Information Services (IIS) Manager**. Klicken Sie dann mit der rechten Maustaste auf die gewünschte Website, und wählen Sie **Neu ► Virtuelles Verzeichnis**.

b. Geben Sie im **Assistenten zum Erstellen von virtuellen Verzeichnissen** den Alias **MESynchAgent** für das virtuelle Verzeichnis ein, und klicken Sie auf **Weiter**.

c. Legen Sie einen Pfad fest, unter dem der Inhalt dieses virtuellen Verzeichnisses gespeichert werden soll, und klicken Sie auf **Weiter**.

HINWEIS: Merken Sie sich den konfigurierten Pfad für eine spätere Verwendung.

d. Aktivieren Sie die Kontrollkästchen **Lesen** und **Schreiben**, und deaktivieren Sie alle anderen Kontrollkästchen. Klicken Sie auf **Weiter** und anschließend auf **Fertig stellen**.

e. Klicken Sie mit der rechten Maustaste auf das virtuelle Verzeichnis **MESynchAgent**, und wählen Sie **Eigenschaften** aus.

f. Wechseln Sie zur Registerkarte **Verzeichnissicherheit**, und klicken Sie in der Gruppe **Authentifizierung und Zugriffssteuerung** auf **Bearbeiten**.

g. Aktivieren Sie in der Gruppe **Authentifizierter Zugriff** das Kontrollkästchen **Standardauthentifizierung**, und legen Sie die **Standarddomäne** und den **Bereich** für Benutzername und Kennwort fest, die von Slave-Rechnern für die Authentifizierung verwendet werden sollen.

HINWEIS: Alle anderen Kontrollkästchen dürfen nicht aktiviert sein.

h. Klicken Sie auf **OK**.

i. Aktivieren Sie auf der Registerkarte **BITS-Servererweiterungen** das Kontrollkästchen **Datenübertragung in dieses virtuelle Verzeichnis durch Clients zulassen**.

j. Klicken Sie auf **OK**, um den Eigenschaftsdialog des virtuellen Verzeichnisses zu schließen.

8.2.3 Schritt 2: Konfigurieren des Master-Servers

1. Klicken Sie auf **Start ► GFI MailEssentials ► GFI MailEssentials Anti-Spam Synchronization Agent**, und klicken Sie dann mit der rechten Maustaste auf den Knoten **Anti-Spam Synchronization Agent ► Konfiguration** sowie auf **Eigenschaften**.

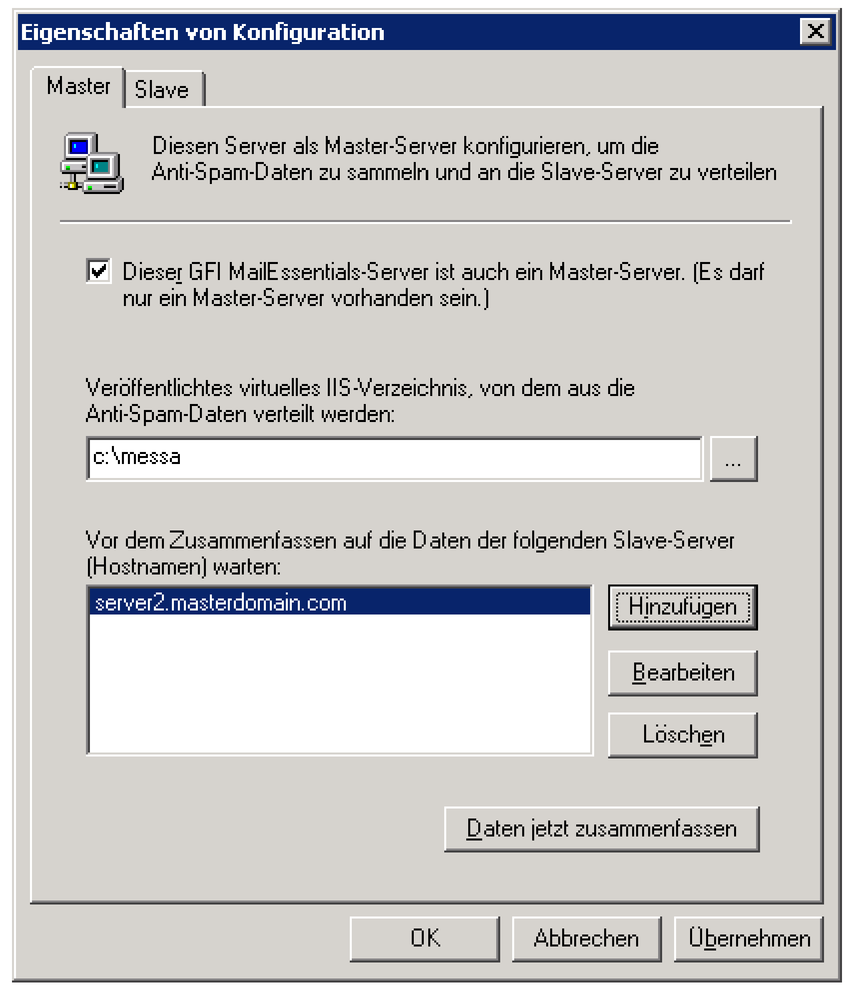


Bild 83 - Konfiguration eines Master-Servers

2. Aktivieren Sie auf der Registerkarte **Master** das Kontrollkästchen **Dieser GFI MailEssentials-Server ist auch ein Master-Server**, und geben Sie den vollständigen Pfad des Ordners ein, in dem der Inhalt des virtuellen Verzeichnisses **MESynchAgent** gespeichert werden soll.

3. Klicken Sie auf **Hinzufügen**, und geben Sie im Bearbeitungsfeld **Server** den Hostnamen des Slave-Servers ein. Klicken Sie auf **OK**, um den Server der Liste hinzuzufügen. Wiederholen Sie diesen Schritt, um alle konfigurierten Slave-Server hinzuzufügen.

HINWEIS 1: Alle Computer, die der Liste hinzugefügt werden, müssen als Slave-Server konfiguriert werden. Andernfalls kann der Anti-Spam Synchronisations-Agent des Master-Servers die Anti-Spam-Daten nicht zusammenführen.

HINWEIS 2: Ein Master-Server kann gleichzeitig auch Slave-Server sein. In diesem Fall führt der Server seine eigenen Anti-Spam-Einstellungen mit den hochgeladenen Einstellungen der anderen Slave-Server zusammen. Damit diese Option funktioniert, müssen Sie den Master-Server-Host-Namen ebenfalls zur Liste der Slave-Server hinzufügen. Weitere Informationen finden Sie im Abschnitt Schritt 3: Konfiguration eines Slave-Servers in diesem Handbuch.

4. Wählen Sie bei Bedarf einen Slave-Server aus der Liste, und klicken Sie auf die Schaltfläche **Bearbeiten** oder **Löschen** um diesen zu bearbeiten oder zu löschen.

5. Klicken Sie auf die Schaltfläche **OK** um die Einstellungen zu speichern.

8.2.4 Schritt 3: Konfiguration eines Slave-Servers

Wichtige Hinweise

1. Zur Konfiguration eines Servers als Slave-Server muss dieser folgende Systemspezifikationen erfüllen:

- Microsoft Windows Server 2008

» Microsoft Windows Server 2003 - Wir empfehlen Ihnen, das BITS 2.0 Client-Update über folgenden Link von Microsoft herunterzuladen:

http://www.microsoft.com/downloads/details.aspx?familyid=3FD31F05-D091-49B3-8A80-BF9B83261372&displaylang=de

2. Von den Slave-Servern wird automatisch eine Archiv-Datei mit Anti-Spam-Einstellungen in das virtuelle IIS-Verzeichnis auf dem Master-Server hochgeladen. Aus diesem Grund sollten auf den Slave-Servern keine virtuellen Verzeichnisse erstellt werden.

Slave-Server-Konfiguration

1. Klicken Sie auf **Start** ► **GFI MailEssentials** ► **GFI MailEssentials Anti-Spam Synchronization Agent**.

2. Klicken Sie mit der rechten Maustaste auf den Knoten **Anti-Spam Synchronization Agent** ► **Konfiguration** und dann auf **Eigenschaften**.

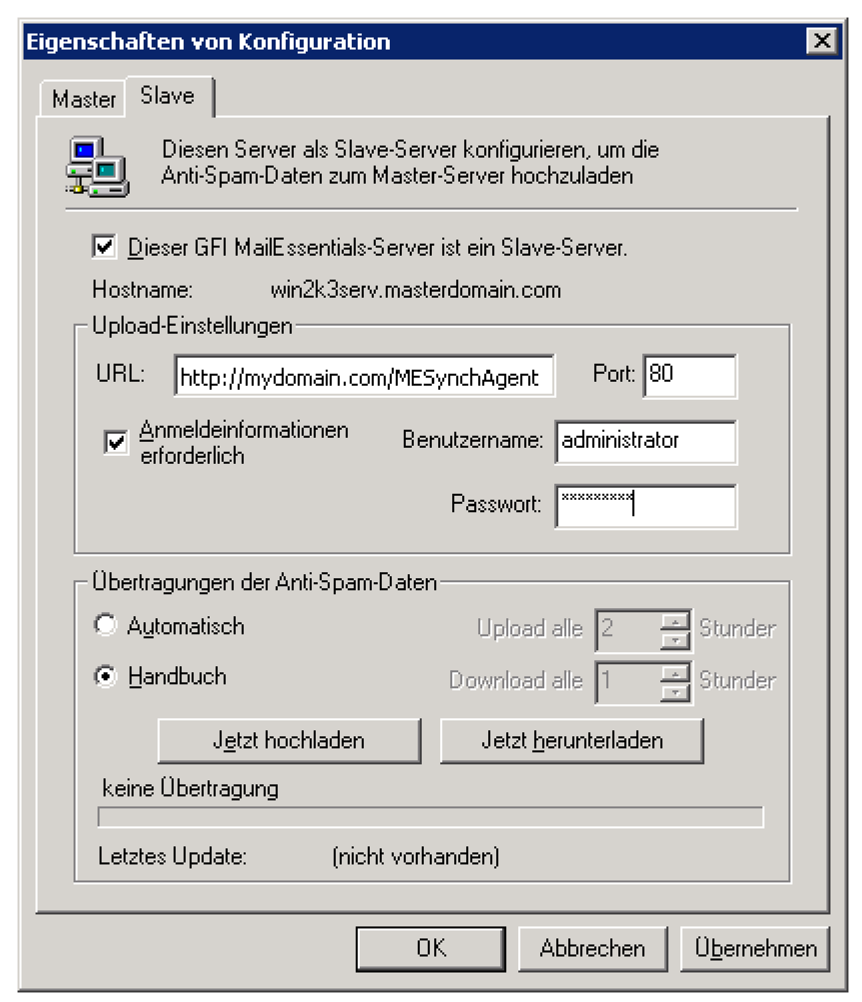


Bild 84 - Konfiguration eines Slave-Servers

3. Aktivieren Sie auf der Registerkarte **Slave** das Kontrollkästchen **Dieser GFI MailEssentials-Server ist ein Slave-Server**.

4. Geben Sie im Feld **URL** die vollständige URL für das virtuelle Verzeichnis auf dem Master-Server im folgenden Format ein:

`http://< Domänenname des Master-Servers>/MESynchAgent`

» **Beispiel:** `http://mydomain.com/MESynchAgent`

5. Geben Sie in dem Feld **Port** den Port an, den der Master-Server für die HTTP-Kommunikation verwendet.

HINWEIS: Voreingestellt ist der Port 80, der Standard-Port für HTTP.

6. Klicken Sie in das Kontrollkästchen **Authentifizierungsdaten erforderlich**, und geben Sie Benutzernamen und Kennwort zur Authentifizierung bei dem Master-Server ein.

7. Wählen Sie:

- **Manuell -** Die Archivdatei mit den Anti-Spam-Einstellungen manuell herunterladen und hochladen. Klicken Sie auf die Schaltfläche **Jetzt hochladen**, wenn Sie die Anti-Spam-Einstellungen des Slave-Servers zum Master-Server hochladen wollen. Klicken Sie auf die Schaltfläche **Jetzt herunterladen**, wenn Sie die aktualisierte, zusammengeführte Datei mit den Anti-Spam-Einstellungen vom Master-Server herunterladen wollen.

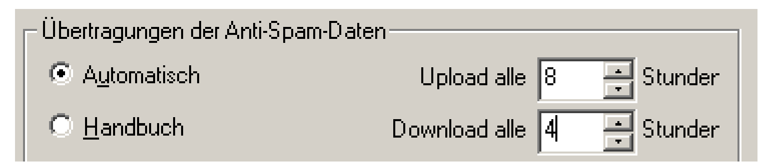


Bild 85 - Stundeneinstellung für das Hochladen/Herunterladen

- **Automatisch -** Konfiguriert die Anti-Spam-Synchronisation so, dass sie automatisch ausgeführt wird. Geben Sie in dem Feld **Hochladen alle** das Hochladeintervall in Stunden an; diese Einstellung legt fest, wie oft der Slave-Server seine Anti-Spam-Einstellungen zum Master-Server hochlädt. Geben Sie in dem Feld **Herunterladen alle** an, wie oft der Slave-Server auf dem Master-Server nach Aktualisierungen suchen und diese herunterladen soll.

HINWEIS: Das Stundenintervall für das Hochladen und Herunterladen dürfen Sie nicht auf den gleichen Wert einstellen. Für das Stundenintervall können Sie einen beliebigen Wert zwischen 1 und 240 Stunden wählen. Wir empfehlen Ihnen, das Intervall zum Herunterladen auf einen kleineren Wert einzustellen als das Intervall für das Hochladen und für alle konfigurierten Slave-Server die gleichen Intervalleinstellungen zu verwenden.

- **Beispiel:** Beispielsweise können Sie das Intervall zum Herunterladen auf drei Stunden und das Intervall zum Hochladen auf vier Stunden einstellen. Auf diese Weise werden Dateien öfter heruntergeladen als hochgeladen.

8. Klicken Sie auf die Schaltfläche **OK** um die Einstellungen zu speichern.

8.3 Exportieren und Importieren von GFI MailEssentials-Einstellungen

GFI MailEssentials beinhaltet ein Import-/Export-Tool für Konfigurationseinstellungen, so dass Einstellungen für andere Installationen von GFI MailEssentials exportiert werden können.

8.3.1 Schritt 1: Exportieren Sie die vorhandenen Konfigurationseinstellungen für GFI MailEssentials

GFI MailEssentials enthält zwei Verfahren zum Export der Konfigurationseinstellungen:

- **Exportieren über die Benutzeroberfläche**
- **Exportieren von Einstellungen über die Befehlszeile**

Exportieren über die Benutzeroberfläche

1. Halten Sie die folgenden GFI MailEssentials-Dienste an:

- GFI MailEssentials Scan-Engine
- GFI MailEssentials Managed Attendant-Dienst

2. Öffnen Sie das Stammverzeichnis von GFI MailEssentials und führen Sie die Datei **meconfigmgr.exe** aus.

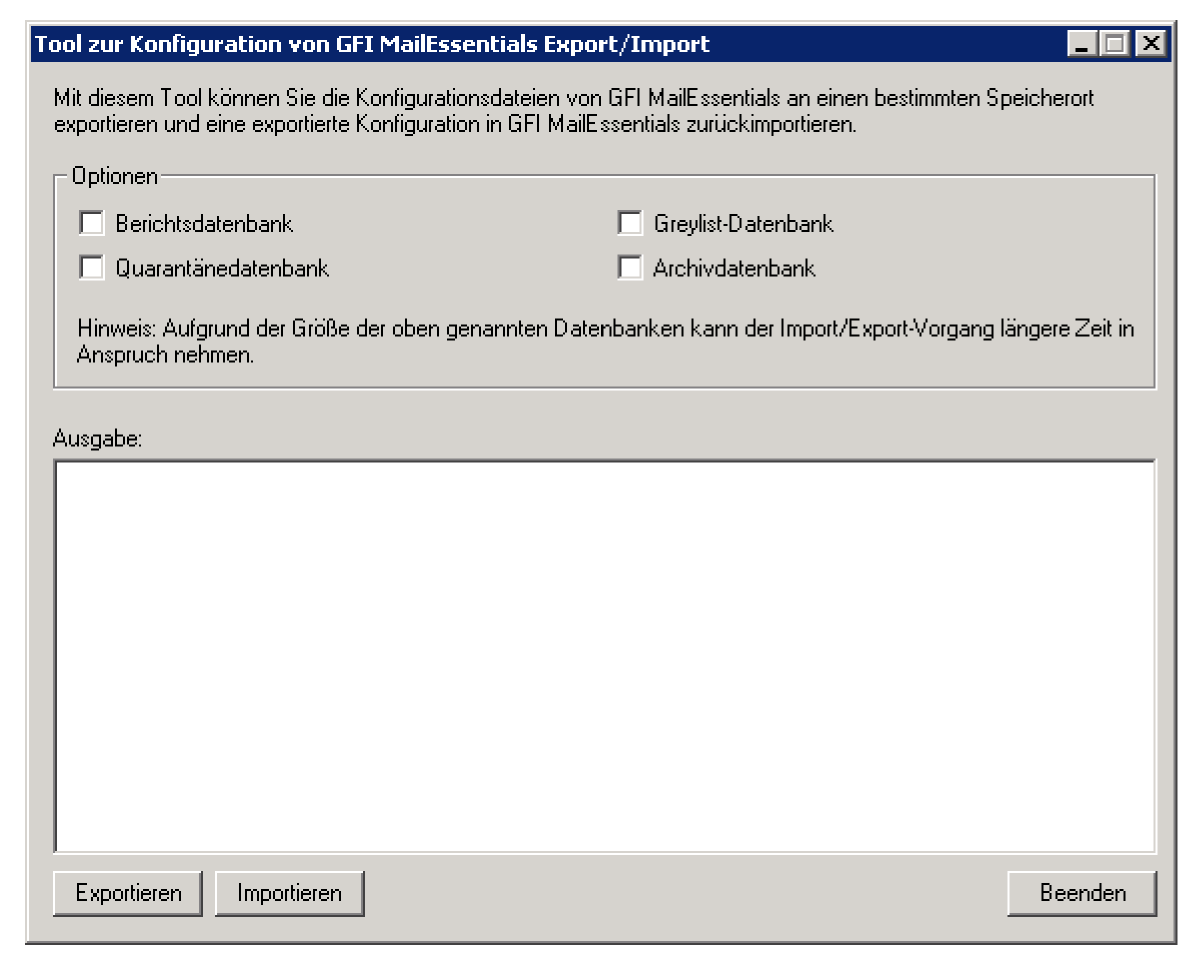


Bild 86 - Konfiguration des GFI MailEssentials Export/Import-Tools

3. (Optional) In GFI MailEssentials können neben Konfigurationseinstellungen auch andere Datenbanken exportiert werden. Wählen Sie die zu exportierenden Datenbanken aus:

» Berichtsdatenbank

» Quarantänedatenbank

» Greylist-Datenbank

» Archivdatenbank

HINWEIS: Die Dauer des Exportvorgangs hängt von der Größe der Datenbank ab.

4. Klicken Sie auf die Schaltfläche **Exportieren**. Wählen Sie in dem Dialog **Nach Ordner Suchen** einen Ordner aus, in den Sie die Konfigurationseinstellungen von GFI MailEssentials exportieren können, und klicken Sie auf **OK**.

5. Klicken Sie nach dem Abschluss auf die Schaltfläche **Beenden**.

6. Starten Sie die Dienste erneut, die Sie in Schritt 1 angehalten haben.

Exportieren von Einstellungen per Befehlszeile

1. Halten Sie die folgenden GFI MailEssentials-Dienste an:

» GFI MailEssentials Scan-Engine

» GFI MailEssentials Managed Attendant-Dienst

2. Öffnen Sie eine Befehlszeile, und suchen Sie nach dem Installationshauptordner von GFI MailEssentials.

3. Geben Sie Folgendes ein:

```
meconfigmgr /export:”c:\MailEssentials Settings” /verbose /replace
```

HINWEIS: Ersetzen Sie “C:\MailEssentials Settings” durch den gewünschten Zielpfad.

```
meconfigmgr.exe /export:"c:\MailEssentials Settings" /verbose /replace
[C:\Program Files\GFI\MailEssentials\config.mdb] wird kopiert -> [c:\MailEssentials Settings\config.mdb]
Fertig
[C:\Program Files\GFI\MailEssentials\autowhitelist.mdb] wird kopiert -> [c:\MailEssentials Settings\autowhitelist.mdb]
Fertig
[C:\Program Files\GFI\MailEssentials\Data\weights.bsp] wird kopiert -> [c:\MailEssentials Settings\weights.bsp]
Fertig
[C:\Program Files\GFI\MailEssentials\userlist.mdb] wird kopiert -> [c:\MailEssentials Settings\userlist.mdb]
Fertig
[C:\Program Files\GFI\MailEssentials\pop2exchange.xml] wird kopiert -> [c:\MailEssentials Settings\pop2exchange.xml]
Fertig
[C:\Program Files\GFI\MailEssentials\spamord.xml] wird kopiert -> [c:\MailEssentials Settings\spamord.xml]
Fertig
[C:\Program Files\GFI\MailEssentials\Data\reports.mdb] wird kopiert -> [c:\MailEssentials Settings\reports.mdb]
Fertig
Fertig_
```

Bild 87 - Exportieren von Einstellungen über die Befehlszeile

- Der Parameter **/Verbose** weist das Tool an, beim Kopieren der Dateien den Arbeitsfortschritt anzuzeigen.
- Der Parameter **/Replace** weist das Tool an, vorhandene Dateien im Zielordner zu überschreiben.

4. Starten Sie die Dienste erneut, die Sie in Schritt 1 angehalten haben.

8.3.2 Schritt 2: Kopieren der exportierten Einstellungen

1. Kopieren Sie manuell den Ordner, in den die Konfigurationseinstellungen exportiert wurden.
2. Fügen Sie den Ordner auf dem Rechner ein, wo die Einstellungen importiert werden sollen.

8.3.3 Schritt 3: Importieren Sie die Einstellungen in die neue Installation von GFI MailEssentials

GFI MailEssentials bietet zwei Verfahren zum Import der Konfigurationseinstellungen:

- Importieren über die Benutzeroberfläche
- Importieren über die Befehlszeile

WICHTIG: Beim Importieren von Einstellungen werden die bestehenden GFI MailEssentials-Einstellungen von den importierten Dateien überschrieben. Dadurch ist wahrscheinlich eine Neukonfiguration von bestimmten Netzwerkeinstellungen und Spam-Aktionen erforderlich.

Importieren per Benutzeroberfläche

1. Halten Sie die folgenden Dienste an:

- GFI-Listenserver
- GFI MailEssentials Enterprise Transfer-Dienst
- GFI MailEssentials Legacy Attendant-Dienst
- GFI MailEssentials Managed Attendant-Dienst
- GFI MailEssentials Scan-Engine
- GFI POP2Exchange
- IIS Admin-Dienst

2. Öffnen Sie das Stammverzeichnis von GFI MailEssentials und führen Sie die Datei **meconfigmgr.exe** aus.

3. (Optional) In GFI MailEssentials können neben Konfigurationseinstellungen auch andere Datenbanken importiert werden. Wählen Sie die zu importierenden Datenbanken aus:

- Berichtsdatenbank
- Quarantänedatenbank
- Greylist-Datenbank
- Archivdatenbank

HINWEIS: Die Dauer des Importvorgangs hängt von der Größe der Datenbank ab.

4. Klicken Sie auf **Importieren**, wählen Sie den Ordner mit den GFI MailEssentials-Importdaten aus, und klicken Sie auf **OK**.

WARNUNG: Beim Importvorgang werden die Installationsdateien mit den Dateien dieses Ordners überschrieben.

5. Importierte Einstellungen könnten nicht mit dieser GFI MailEssentials-Installation kompatibel sein, und einige Einstellungen müssen wahrscheinlich neu konfiguriert werden. Dies geschieht, wenn sich bestimmte Netzwerkparameter (wie DNS-Einstellungen, Domänenlisten und Perimeterserver) von dem Server unterscheiden, von dem die Einstellungen exportiert wurden. Es wird empfohlen, auf **Ja** zu klicken, um den Nachinstallationsassistenten von GFI MailEssentials zu starten. Dieser konfiguriert wichtige Einstellungen neu. Weitere Informationen zu den Konfigurationsschritten im Nachinstallationsassistenten finden Sie in „GFI MailEssentials - Erste Schritte“ unter **http://www.gfi.com/mes/manual**.

HINWEIS: Weitere Informationen zu Einstellungen, die nach dem Import geprüft werden sollten, finden Sie unter:

http://kbase.gfi.com/showarticle.asp?id=KBID003956.

6. Klicken Sie nach Abschluss auf die Schaltfläche **Beenden**.

7. Starten Sie die Dienste erneut, die Sie in Schritt 1 angehalten haben.

Importieren per Befehlszeile

1. Halten Sie die folgenden Dienste an:

- GFI-Listenserver
- GFI MailEssentials Enterprise Transfer-Dienst
- GFI MailEssentials Legacy Attendant-Dienst
- GFI MailEssentials Managed Attendant-Dienst
- GFI MailEssentials Scan-Engine
- GFI POP2Exchange
- IIS Admin-Dienst

2. Öffnen Sie eine Befehlszeile, und suchen Sie nach dem Hauptinstallationsordner von GFI MailEssentials.

3. Geben Sie Folgendes ein:

```
meconfigmgr /import:”c:\MailEssentials Settings” /verbose /replace
```

Hinweis: Ersetzen Sie “C:\MailEssentials Settings” durch den gewünschten Quellpfad.

WARNUNG: Beim Importvorgang werden die Installationsdateien mit den Dateien dieses Ordners überschrieben.

```
meconfigmgr.exe /import:"c:\MailEssentials Settings" /verbose /replace
[c:\MailEssentials Settings\config.mdb] wird kopiert -> [C:\Program Files\GFI\MailEssentials\config.mdb]
Datei vorhanden, wurde überschrieben
[c:\MailEssentials Settings\autowhitelist.mdb] wird kopiert -> [C:\Program Files\GFI\MailEssentials\autowhitelist.mdb]
Datei vorhanden, wurde überschrieben
[c:\MailEssentials Settings\weights.bsp] wird kopiert -> [C:\Program Files\GFI\MailEssentials\Data\weights.bsp]
Datei vorhanden, wurde überschrieben
[c:\MailEssentials Settings\userlist.mdb] wird kopiert -> [C:\Program Files\GFI\MailEssentials\userlist.mdb]
Datei vorhanden, wurde überschrieben
[c:\MailEssentials Settings\pop2exchange.xml] wird kopiert -> [C:\Program Files\GFI\MailEssentials\pop2exchange.xml]
Datei vorhanden, wurde überschrieben
[c:\MailEssentials Settings\spamord.xml] wird kopiert -> [C:\Program Files\GFI\MailEssentials\spamord.xml]
Datei vorhanden, wurde überschrieben
[c:\MailEssentials Settings\reports.mdb] wird kopiert -> [C:\Program Files\GFI\MailEssentials\Data\reports.mdb]
Datei vorhanden, wurde überschrieben
==== Importieren... Fertig! ====
==== Überprüfen... ====
Anti-Spam-Aktionspfade werden überprüft...
Konfiguration der Installationspfade von GFI MailEssentials wird überprüft...
Konfiguration der Installationspfade von GFI MailEssentials wird überprüft... Fertig!
==== Überprüfen... Fertig! ====

Fertig_
```

Bild 88 - Importieren von Einstellungen über die Befehlszeile

- Der Parameter **/Verbose** weist das Tool an, den Arbeitsfortschritt beim Kopieren der Dateien wie in der folgenden Abbildung anzuzeigen.
- Der Parameter **/Replace** weist das Tool an, vorhandene Dateien im Zielordner zu überschreiben.

4. Starten Sie die Dienste erneut, die Sie in Schritt 1 angehalten haben.

HINWEIS: Importierte Einstellungen könnten nicht mit dieser GFI MailEssentials-Installation kompatibel sein, und einige Einstellungen müssen wahrscheinlich neu konfiguriert werden. Weitere Informationen finden Sie unter:

http://kbase.gfi.com/showarticle.asp?id=KBID003956.

8.4 Auswahl des virtuellen SMTP-Servers zur Bindung an GFI MailEssentials

Bei mehreren virtuellen SMTP-Servern müssen Sie gegebenenfalls GFI MailEssentials an neue oder andere virtuelle SMTP-Server anbinden.

HINWEIS: Die Registerkarte Virtuelle SMTP-Server-**Anbindungen** wird nicht angezeigt, wenn Sie GFI MailEssentials auf einen Computer mit Microsoft Exchance Server 2007/2010 installiert haben.

8.4.1 Anbindungen von GFI MailEssentials an virtuelle SMTP-Server

1. Klicken Sie mit der rechten Maustaste auf den Knoten **Allgemein** ► **Allgemein Einstellungen**, dann auf **Eigenschaften** und die Registerkarte **Anbindungen**.



Bild 89 - Anbindungen für den virtuellen SMTP-Server

2. Klicken Sie in der Liste **Name des virtuellen SMTP-Servers** in das Kontrollkästchen des virtuellen SMTP-Servers um die Anbindung mit GFI MailEssentials herzustellen.

3. Klicken Sie auf die Schaltfläche **OK** um die Konfiguration zu übernehmen.

HINWEIS: Die Konfiguration von GFI MailEssentials verlangt einen Neustart der Dienste wie beispielsweise des IIS SMTP-Dienstes, damit die neuen Einstellungen wirksam werden. Klicken Sie auf die Schaltfläche **Ja** um die Dienste neu zu starten.

8.5 Deaktivieren/Aktivieren des E-Mail-Verarbeitung

Mit Deaktivierung des Scannens deaktivieren Sie alle Schutzfunktionen von GFI MailEssentials, sodass alle E-Mails, auch Spam-Mails, in die Benutzerpostfächer gelangen.

So aktivieren/deaktivieren Sie das Scannen von E-Mails mit GFI MailEssentials:

1. Klicken Sie auf **Start** ► **Programme** ► **GFI MailEssentials** ► **GFI MailEssentials Switchboard**.

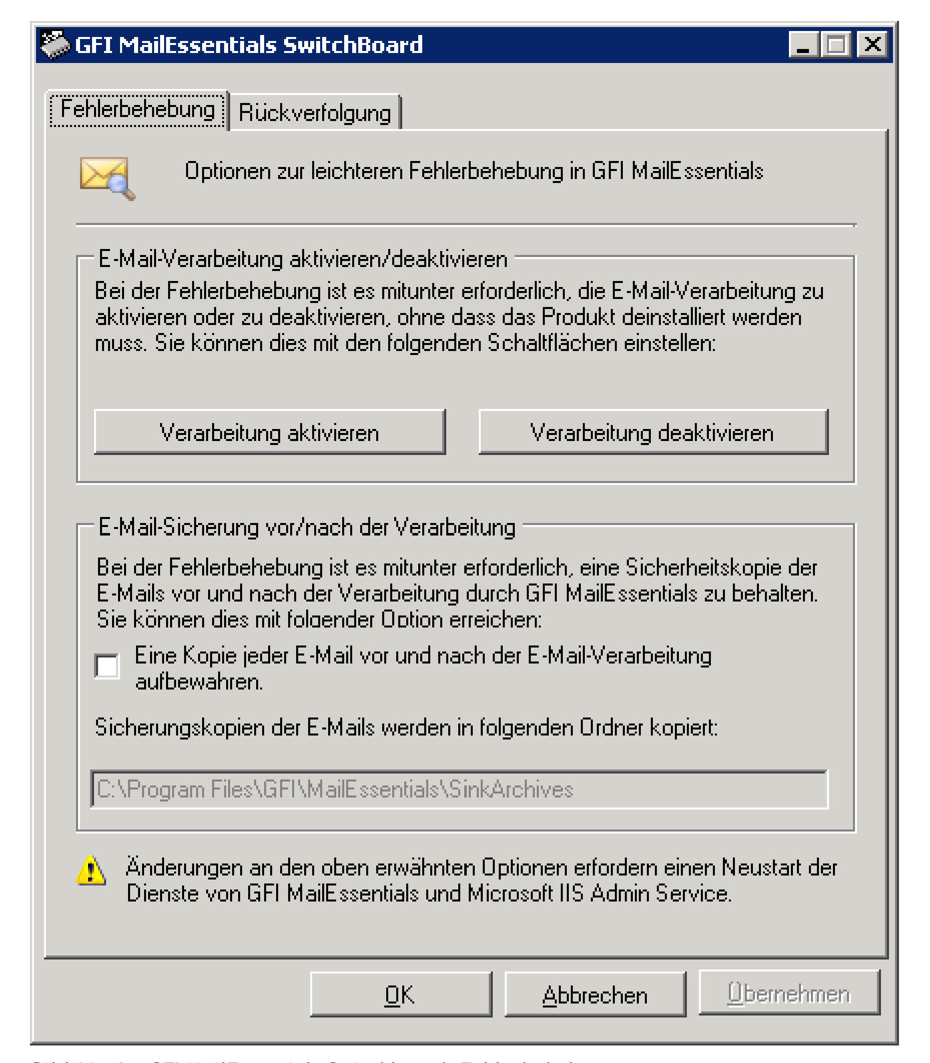


Bild 90 - Im GFI MailEssentials Switchboard: Fehlerbehebung

2. Klicken Sie auf die Registerkarte **Fehlerbehebung**:

- und dann auf **Verarbeitung deaktivieren**, um das Scannen von E-Mails zu deaktivieren.
- und dann auf **Verarbeitung aktivieren**, um das Scannen von E-Mails zu aktivieren.

Der Scan von E-Mails kann durch einen Befehl in der Befehlszeile aktiviert und deaktiviert werden. Weitere Informationen finden Sie unter:

http://kbase.gfi.com/showarticle.asp?id=KBID003468.

8.6 Rückverfolgung

GFI MailEssentials kann Protokolle zur Fehlerbehebung erstellen. Ist diese Option aktiviert, speichert GFI MailEssentials die Aktivitäten in dem Ordner "DebugLogs" im Installationsordner von GFI MailEssentials. So konfigurieren Sie die Rückverfolgung:

1. Klicken Sie auf **Start** ► **Programme** ► **GFI MailEssentials** ► **GFI MailEssentials Switchboard.**

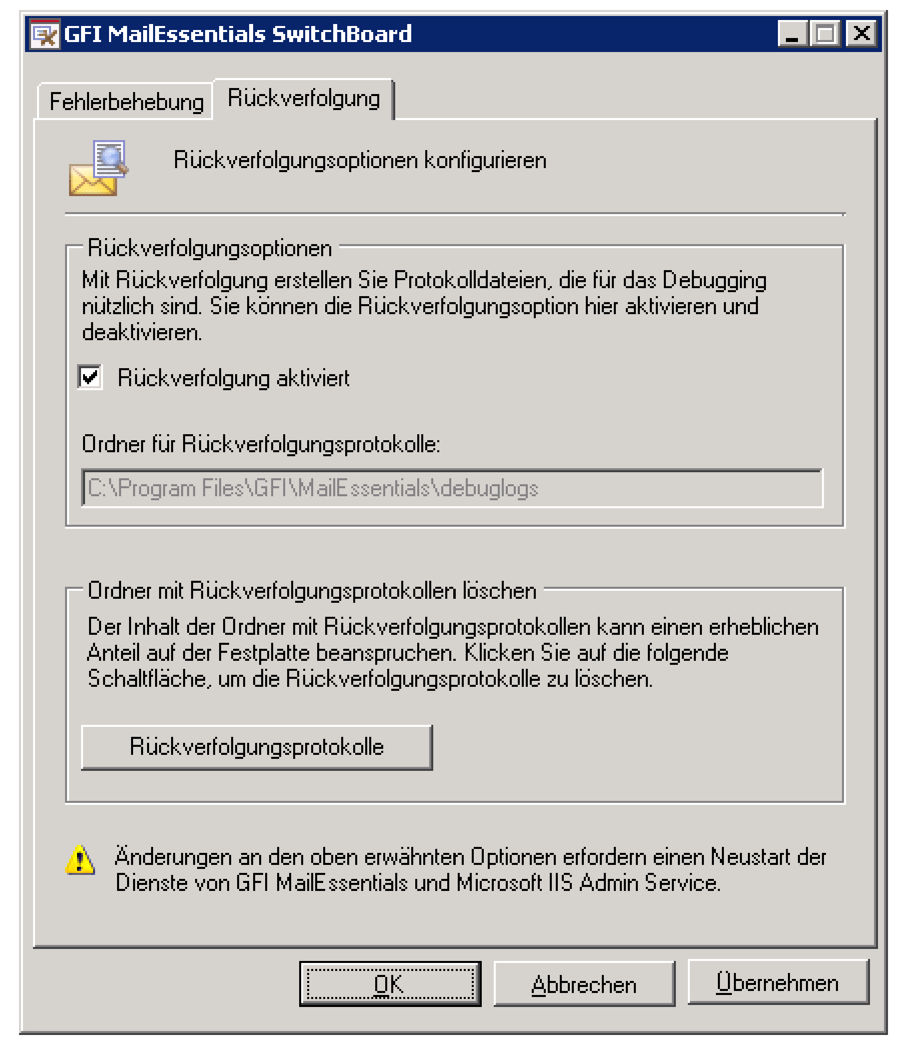


Bild 91 - Rückverfolgung

2. Klicken Sie auf die Registerkarte **Rückverfolgung** und konfigurieren Sie folgende Optionen:

- Markieren oder demarkieren Sie das Kontrollkästchen **Rückverfolgung aktiviert**, um die Rückverfolgung zu aktivieren oder zu deaktivieren. Diese Option ist standardmäßig aktiviert.
- Klicken **Rückverfolgungsprotokolle**, um alle Protokolle zu löschen.

E-Mail-Sicherung vor/nach der Verarbeitung

WICHTIGER HINWEIS: Wir empfehlen unbedingt, diese Option deaktiviert zu lassen und nur für die Fehlerbehebung nach Anleitung von Fachpersonal zu verwenden.

Markieren/demarkieren Sie das **Kontrollkästchen "Eine Kopie jeder E-Mail vor und nach der E-Mail-Verarbeitung behalten**", um eine Kopie jeder verarbeiteten E-Mail in dem Ordner "SinkArchives" im Installationsordner von GFI MailEssentials.

8.7 Remote-Befehle

Remote-Befehle erleichtern das Hinzufügen von Domänen oder E-Mail-Adressen zur Spam-Blockliste sowie eine Aktualisierung des Bayes-Filters SPAM oder HAM (zulässigen E-Mails).

Remote-Befehle senden eine E-Mail an GFI MailEssentials. Wenn Sie eine E-Mail an rcommands@mailessentials.com (konfigurierbar) senden, erkennt GFI MailEssentials, dass die E-Mail Remote-Befehle enthält und verarbeitet die Befehle.

Mit Remote-Befehlen können Sie folgende Aufgaben ausführen:

1. Sie können SPAM oder HAM für das Bayes-Modul hinzufügen.

2. Sie können entweder Keywords für die Prüfung der Betreffzeile oder des Nachrichtentextes hinzufügen.

3. Sie können E-Mail-Adressen zum Blockliste-Filter hinzufügen.

8.7.1 Konfigurieren von Remote-Befehlen

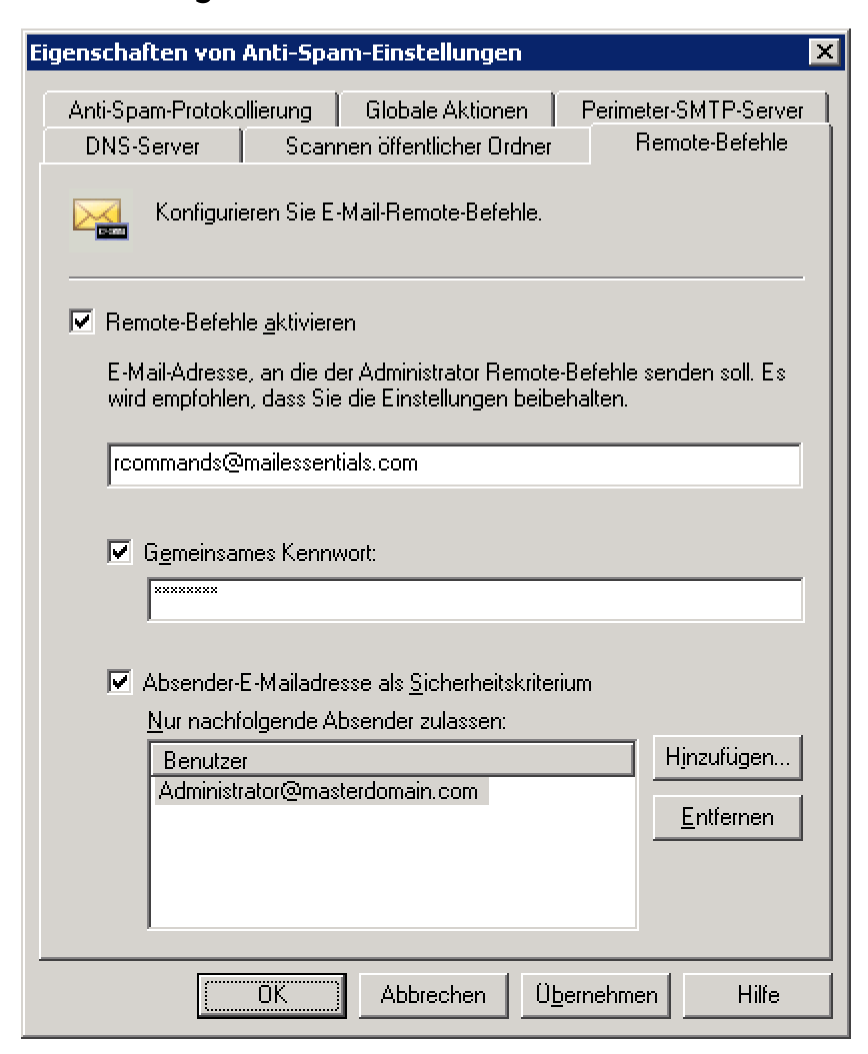


Bild 92 - Remote-Befehle, Konfiguration

1. Klicken Sie mit der rechten Maustaste auf **Anti-Spam ► Anti-Spam-Einstellungen**, dann auf **Eigenschaften**, klicken Sie auf die Registerkarte **Remote-Befehle** und dann in das Kontrollkästchen **Remote-Befehle aktivieren**.

2. Bearbeiten Sie die E-Mail-Adresse, an die die Remote-Befehle gesendet werden sollen.

HINWEIS: Die E-Mail-Adresse sollte keine lokale Domäne sein. Wir empfehlen als Adresse rcommands@mailessentials.com. Ein Postfach für die konfigurierte Adresse muss nicht existieren, aber der Domänenteil der Adresse muss mit einer real existierenden E-Mail-Adressen-Domäne übereinstimmen, die bei einer MX-Eintragssuche über DNS ein positives Ergebnis liefert.

3. Optional können Sie einige Basissicherheitsfunktionen für Remote-Befehle konfigurieren:

- Konfigurieren Sie ein gemeinsames Kennwort, das in der E-Mail enthalten sein soll. Weitere Informationen finden Sie unter Verwenden von Remote-Befehlen in diesem Handbuch.
- Konfigurieren Sie außerdem, welche Benutzer E-Mails mit Remote-Befehlen versenden dürfen.

8.7.2 Verwenden von Remote-Befehlen

Remote-Befehle können von einem E-Mail-Client innerhalb der Domäne per E-Mail an GFI MailEssentials gesendet werden. Bedingungen zum Senden von Remote-Befehlen:

- Die E-Mail muss im Klartextformat sein.
- Der Betreff der E-Mail ist leer.

» Die folgende Syntax muss für alle Befehle verwendet werden:

```
<Befehlsname>: <Parameter1>, <Parameter2>, <Parameter3>, … ;
```

Beispiel: ADDSUBJECT: Sex, Porno, Spam;

» Im Textkörper einer E-Mail kann mehr als ein Befehl verwendet werden. Alle Befehle müssen durch ein Semikolon (;) voneinander getrennt sein.

» Falls für Remote-Befehle ein Kennwort festgelegt wird, geben Sie das Kennwort in die erste Zeile gemäß der folgenden Syntax ein:

```
PASSWORD: <gemeinsames Passwort>;
```

» Bei jedem Befehlsnamen muss die Groß-/Kleinschreibung beachtet werden. Es wird empfohlen, nur GROSSSCHREIBUNG zu verwenden.

» Bedingungen wie IF, AND, OR... werden nicht unterstützt.

» Remote-Befehle können nur verwendet werden, um Einträge hinzuzufügen. Sie dienen nicht zum Löschen oder Ändern vorhandener Einträge.

8.7.3 Stichwortbefehle

Verwenden Sie Stichwortbefehle, um Stichwörter oder Stichwortkombinationen in die Textkörper- oder Betrefflisten des Filters zur Stichwortprüfung einzufügen.

Verfügbare Befehle sind:

» **ADDSUBJECT** - Ergänzt Keywords für die Datenbank, die die Keywords in der Betreffzeile prüft.

- **Beispiel:** ADDSUBJECT: sex, porn, spam;

» **ADDBODY** - Ergänzt Keywords in der Datenbank, die nach Keywords im Nachrichtentext sucht.

- **Beispiel:** ADDBODY: free, “100% free”, “absolutely free”;

HINWEIS: Wenn Sie Phrasen konfigurieren, die aus mehreren Wörtern bestehen, schließen Sie die Phrasen in doppelte Anführungszeichen ein (“ ”).

8.7.4 Blockliste-Befehle

Mit Blockliste-Befehlen ergänzen Sie eine einzelne E-Mail-Adresse oder eine komplette Domäne in der benutzerdefinierten Blockliste.

Verfügbare Befehle sind:

» **ADDBLIST:** <email>;

- **Beispiel:** ADDBLIST: user@somewhere.com;

HINWEIS 1: Fügen Sie eine komplette Domäne in der Blockliste hinzu, indem Sie ein Ersatzzeichen vor der Domäne einfügen

» **Beispiel:** ADDBLIST: *@Domäne.com.

HINWEIS 2: Aus Sicherheitsgründen darf nur ein Befehl ADDBLIST in einer E-Mail enthalten sein, und es darf nur eine Adresse als Befehlsparameter angegeben sein. Der Parameter ist entweder eine Benutzer-E-Mail oder eine Domäne:

» **Beispiel:** spammer@spam.com oder *@spammers.org.

HINWEIS 3: Platzhalter können in Domänennamen nicht verwendet werden.

» **Beispiel:** *@*.domäne.com wird als ungültig zurückgewiesen.

8.7.5 Bayes-Filter-Befehle

Ergänzen Sie Spam-Mails oder zulässige E-Mails (HAM) in der Bayes-Filter-Datenbank. Verfügbare Befehle sind:

- **ADDASSPAM** - weist den Bayes-Filter an, die E-Mail als Spam-Mail einzustufen.
- **ADDASGOODMAIL** - weist den Bayes Bayes-Filter an, die E-Mail als HAM einzustufen.

HINWEIS: Für diese Befehle gibt es keine Parameter - der Parameter ist der Rest der E-Mail.

Beispiele

- **Beispiel 1**- Bei diesem Beispiel ergänzt der Benutzer spammer@spamhouse.com in der Blockliste und fügt einige Keywords in der Datenbank hinzu, die nach Keywords in der Betreffzeile sucht.

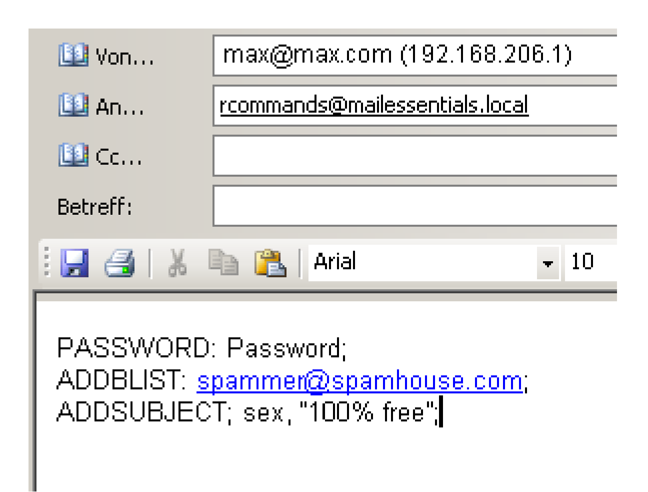


Bild 93 - Hinzufügen einer E-Mail-Adresse zur Blockliste und Keywords

- **Beispiel 2** - Der gleiche Befehl kann mehr als einmal angegeben werden (in diesem Fall ADDBODY). Das Ergebnis ist kumulativ und in diesem Fall werden folgende Keywords in der Datenbank hinzugefügt, die Keywords im Nachrichtentext prüft: sex, 100% free und instant money.

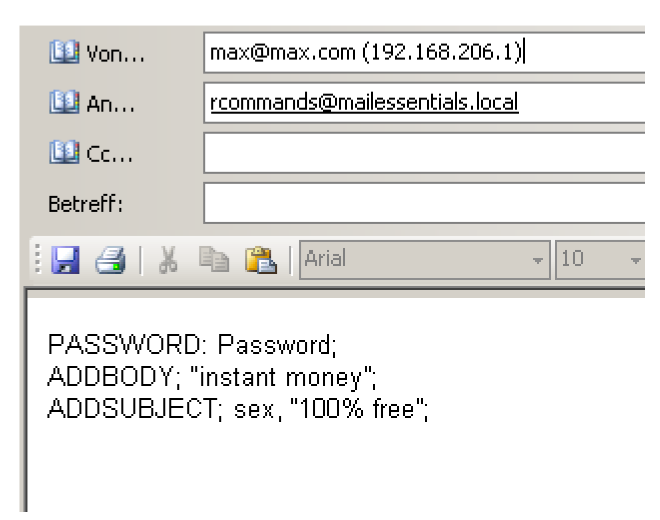


Bild 94 - Mehrmalige Definition des gleichen Befehls

- **Beispiel 3:** Eine Spam-Mail wird mit dem Befehl ADAASSPAM hinzugefügt. Bei diesem Befehl ist ein Doppelpunkt nicht erforderlich - alles unmittelbar nach diesem Befehl wird als Daten behandelt.

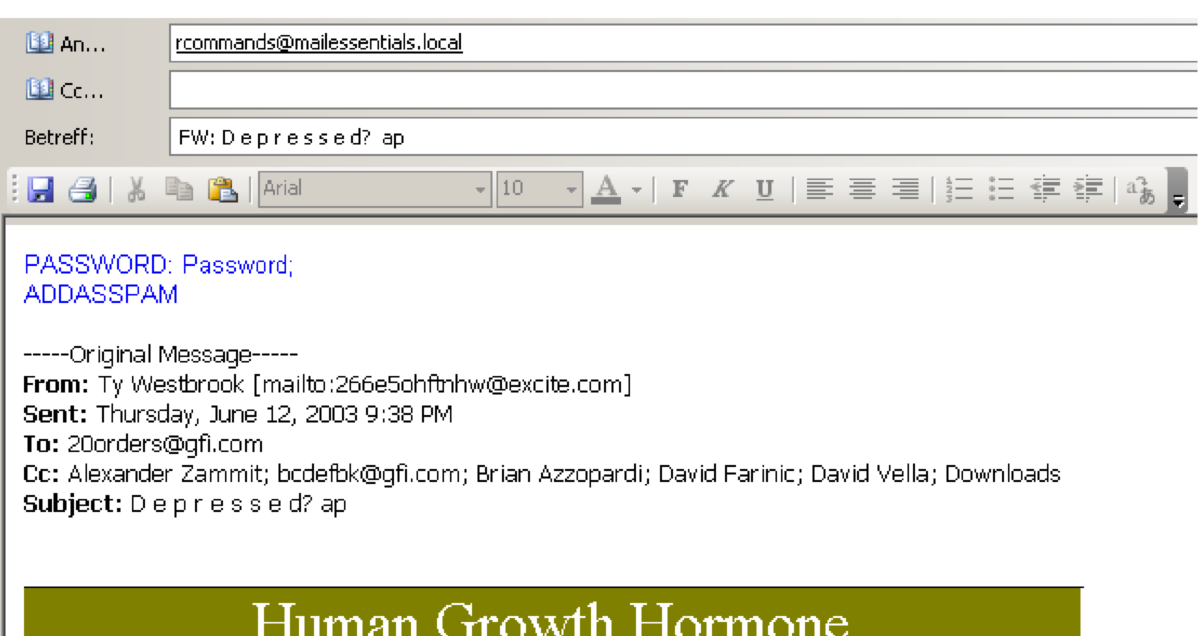


Bild 95 - Hinzufügen von Spam-Mails in der Bayes-Filterdatenbank

» **Beispiel 4** - Wenn das Kontrollkästchen **Gemeinsames Kennwort** nicht aktiviert ist, können Remote-Befehle ohne Kennwort gesendet werden.

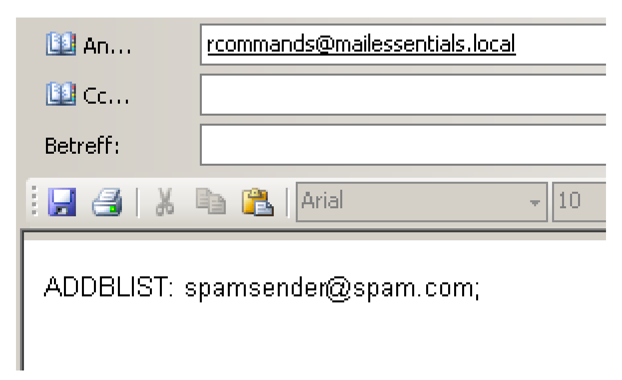


Bild 96 - Senden von Remote-Befehlen ohne Sicherheit

8.7.6 Protokollieren von Remote-Befehlen

Damit Änderungen an der Konfigurationsdatenbank, die über Remote-Befehle vorgenommen wurden, verfolgt werden können, wird jede E-Mail, die mit Remote-Befehlen (selbst wenn die E-Mail mit den Remote-Befehlen ungültig war) in dem Unterordner ADBRProcessed in dem Hauptordner von GFI MailEssentials gespeichert. Der Dateiname in jeder E-Mail wird entsprechend folgendem Format formatiert:

» <Absender_E-Mail_Adresse>_SUCCESS_<Zeitstempel>.eml - bei einer erfolgreichen Bearbeitung.

- <Absender_E-Mail_Adresse>_FAILED_<Zeitstempel>.eml - bei einem Fehler.

HINWEIS: Der Zeitstempel wird formatiert als yyyyddmmhhmmss.

8.8 Verschieben von Spam-E-Mails in den Postfachordner des Benutzers

Wenn GFI MailEssentials auf einem Microsoft Exchange Server installiert ist, speichern Sie Spam-E-Mails entsprechend der Beschreibung im Kapitel Spam-Aktionen - Umgang mit Spam-Mails in diesem Handbuch.

Wenn GFI MailEssentials NICHT auf einem Microsoft Exchange Server installiert ist, können Spam-E-Mails nicht mit der Option "Spam-Aktionen" in einen spezifischen Postfachordner des Benutzers umgeleitet werden. Die E-Mails können jedoch wie im Folgenden beschrieben in das Postfach des Benutzers umgeleitet werden.

8.8.1 Microsoft Exchange Server 2003

GFI MailEssentials enthält einen Regelmanager, der als Spam gekennzeichnete E-Mails automatisch in das Benutzerpostfach verschiebt.

WICHTIGER HINWEIS: Um den Rules Manager zu verwenden, klicken Sie unter **Spam-Aktionen auf die Option "E-Mail mit bestimmtem Text markieren**" und geben einen Kennzeichnungstext an.

Rules Manager auf Microsoft Exchange Server installieren

1. Suchen Sie auf dem Computer mit GFI MailEssentials den Installationsordner von GFI MailEssentials.

2. Kopieren Sie die folgenden Dateien in einen Ordner auf dem Microsoft Exchange Server:

- rulemgmtres.dll
- rulemgmt.exe
- rule.dll
- gfi_log.dll

3. Öffnen Sie auf Microsoft Exchange Server eine Befehlszeile und ändern Sie das Verzeichnis für den Speicherort, in den die Dateien des Rules Manager kopiert wurden.

4. Geben Sie auf der Befehlszeile Folgendes ein: **regsvr32 rule.dll**

5. Klicken Sie zur Bestätigung auf **OK** .

Rules Manager starten

1. Suchen Sie auf dem Microsoft Exchange Server den Ort, an den die Dateien des Rules Manager kopiert wurden und öffnen Sie die Datei **rulemgmt.exe**..

2. Wählen Sie eine Microsoft Outlook Profildatei (MAPI-Profil) aus oder erstellen Sie ein neues Profil für die Anmeldung (nur, wenn Sie den Rules Manager erstmals verwenden).

3. Klicken Sie auf **OK**, um den Rules Manager zu starten.

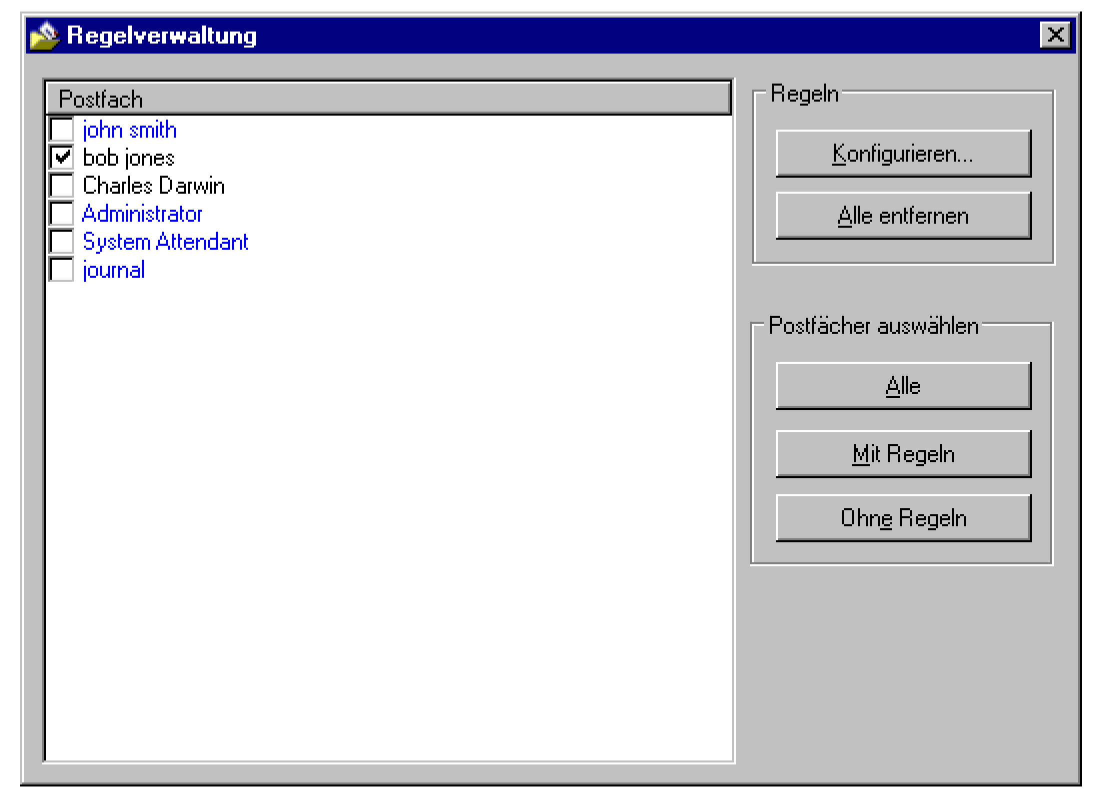


Bild 97 - Der Rules Manager von GFI MailEssentials

4. Das Hauptfenster des Rules Manager zeigt alle auf dem Microsoft Exchange Server aktivierten Postfächer. Die Farbe der Postfächer gibt den Status des betreffenden Postfachs an:

- Blau - Postfach mit konfigurierten Regeln
- Schwarz - Postfach ohne konfigurierte Regeln

Definieren neuer Regeln

1. Markieren Sie die Postfächer, für die Sie eine Regel definieren wollen und klicken Sie auf **Konfigurieren** …, um den Dialog **Globale Regel konfigurieren** zu starten.

HINWEIS 1: Sie können neue Regeln zu Postfächern hinzufügen, die bereits Regeln enthalten.

HINWEIS 2: Wählen Sie mehrere Postfächer aus, um die gleiche Regel für alle Postfächer zu konfigurieren -



Bild 98 - Hinzufügen einer neuen Regel im Rules Manager

2. Geben Sie in dem Textfeld **Regelbedingung** die Kennzeichnung ein, die die Spam-E-Mail durch die Option "Spam-Aktionen" von GFI MailEssentials erhält.

3. Geben Sie die **Regelaktion** ein:

» Klicken Sie auf **Löschen**, um die E-Mail zu löschen, deren Betreff die Regelbedingung enthält.

» Klicken Sie auf **Verschieben in:** , Um eine Spam-E-Mail in einen Ordner des Postfachs zu verschieben. Geben Sie den Ordnerpfad ein, in den die Spam-E-Mail verschoben werden soll. Wenn Sie "**Posteingang\Spam**" angeben, wird ein Spamordner im Posteingangsordner erstellt. Wenn Sie nur "**Spam**" eingeben, wird der Ordner auf der obersten Ebene (gleiche Ebene wie Posteingang) erstellt.

4. Klicken Sie auf **Übernehmen**, um die definierten Regeln zu speichern.

Verwalten mehrerer Regeln

Sie können für das gleiche Postfach mehr als eine Regel definieren.

Beispiel: Mit [Phishing] markierte E-Mails löschen und mit [Spam] gekennzeichnete E-Mails in den Posteingangs-Spamordner verschieben.

1. Doppelklicken Sie auf ein Postfach, um den Regeldialog zu starten.

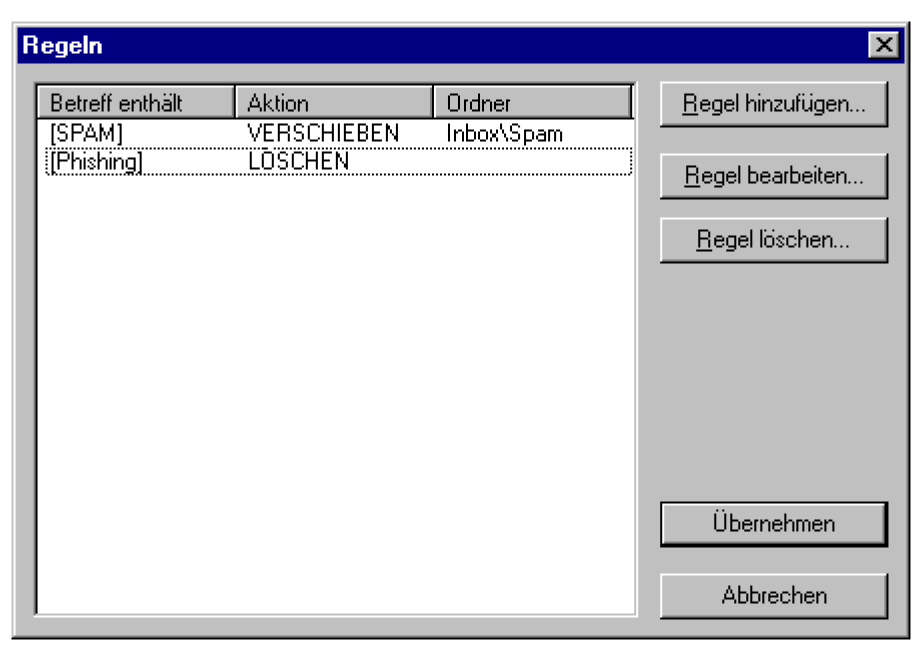


Bild 99 - Liste der Regeln in Rules Manager

2. Es wird eine Liste der für den ausgewählten Posteingang geltenden Regeln angezeigt.

» Klicken Sie auf **Regel hinzufügen**, um eine neue Regel hinzuzufügen.

» Wählen Sie eine Regel aus und klicken Sie auf **Regel bearbeiten**, um die Einstellungen für die ausgewählte Regel zu ändern.

» Wählen Sie ein Regel aus und klicken Sie auf **Regel löschen**, um die ausgewählte Regel zu löschen.

3. Klicken Sie auf **&Übernehmen**, um die Einstellung zu speichern.

8.8.2 Microsoft Exchange 2007/2010

Um Microsoft Exchange 2007/2010 so zu konfigurieren, dass gekennzeichnete E-Mails in den Junk-Postfachordner des Benutzers weitergeleitet werden, müssen Sie eine Transportregel erstellen.

WICHTIGER HINWEIS: Klicken Sie in GFI MailEssentials "Spam-Aktionen" auf die Option **E-Mail mit bestimmtem Text kennzeichnen** . Wenn Sie auf eine andere Aktion klicken, erreichen die als Spam erkannten E-Mails nicht das Postfach des Benutzers, und daher bleiben die konfigurierten Transportregeln unwirksam.

So erstellen Sie eine Transportregel in Exchange 2007/2010:

1. Starten Sie die **Microsoft Exchange Managementkonsole**.

2 Wechseln Sie zum Knoten **Microsoft Exchange ► Organisationskonfiguration ► Hub-Übertragung** und klicken Sie auf die Option **Übertragungsregeln**.

3. Klicken Sie zum Start des Assistenten auf **Neue Transportregel**.

4. Geben Sie für die neue Regel einen Namen ein (beispielsweise GFI MailEssentials Spam) und klicken Sie auf **Weiter** .

5. Wählen Sie in dem Bereich **Bedingungen** die Option **Wenn das Betrefffeld bestimmte Worte enthält aus**.

6. Klicken Sie in dem Bereich **Regel bearbeiten** auf **bestimmte Worte**, um die für die Kennzeichnung verwendeten Worte einzugeben. Geben Sie die in den unter "Spam-Aktionen" definierten Kennzeichnungen für jeden Spamfilter ein und klicken Sie auf **Hinzufügen** (Beispiel: [SPAM]). Klicken Sie auf **OK**, wenn alle Worte hinzugefügt sind und dann auf **Weite**r .

7. Klicken Sie im Bereich "Aktionen" auf die Option **Spam-Konfidenzgrad auf Wert setzen** .

8. Klicken Sie im Bereich **Regel bearbeiten** auf **0** und setzen Sie den Konfidenzgrad auf **9**. Klicken Sie auf **OK** und dann auf **Weiter** .

9. (Optional) Definieren Sie Ausnahmen für diese Transportregeln und klicken Sie dann auf **Weiter** .

10. Klicken Sie auf **Neu**, um eine neue Transportregel zu erstellen.

HINWEIS: Achten Sie darauf, dass der Junk-E-Mail-Ordner für die Benutzerpostfächer aktiviert ist.

Die erstellte Transportregel leitet jetzt alle E-Mails, die die Kennzeichnung von GFI MailEssentials enthalten, in den Junk-E-Mail-Ordner der Benutzer.

9 Problembehandlung & Support

9.1 Einführung

Dieses Kapitel erläutert, wie Probleme bei der Installation von GFI MailEssentials beseitigt werden können. Nutzen Sie die folgenden Informationsquellen in der im Folgenden aufgelisteten Reihenfolge:

1. Dieses Handbuch
2. Die Abschnitte "Häufige Probleme" im Folgenden
3. Die Artikel in der GFI Knowledge Base
4. Gemeinsame Prüfungen
5. Web-Foren
6. Kontakt zum technischen Support von GFI

9.2 Benutzerhandbuch

Nutzen Sie die Informationen in diesem Benutzerhandbuch um zu erkennen, welche Ursachen Probleme bei der Installation von GFI MailEssentials haben könnten. Die Informationskapitel sowie die Kapitel Häufige Probleme enthalten Anleitungen, wie Sie Probleme beseitigen können, die aufgrund menschlicher Fehler oder aufgrund von Fehlkonfigurationen auftreten.

9.3 Häufige Probleme

Die Liste häufiger Probleme im Folgenden enthält Probleme, die andere Benutzer häufiger bei der Nutzung von GFI MailEssentials festgestellt haben.

9.4 Umgang mit Spam

FESTGESTELLTES PROBLEM	LÖSUNG
1. Das Dashboard zeigt, dass keine E-Mail verarbeitet wird: Es werden nur eingehende oder nur ausgehende E-Mails verarbeitet.	1. Kontrollieren Sie, dass das Scannen von E-Mails durch GFI MailEssentials nicht deaktiviert wurde. Weitere Informationen, wie Sie den Scan-Vorgang starten, finden Sie in Kapitel Deaktivieren/Aktivieren des E-Mail-Verarbeitung in diesem Handbuch. 2. Kontrollieren Sie, ob mehrere virtuelle Microsoft IIS SMTP-Server IIS SMTP vorhanden sind, und ob GFI MailEssentials an den richtigen virtuellen Server gebunden ist. 3. MX-Eintrag für die Domäne nicht richtig konfiguriert. Kontrollieren Sie, ob der MX-Eintrag auf die IP-Adresse des Servers zeigt, auf dem GFI MailEssentials gestartet ist. 4. Wenn eingehende E-Mails durch ein anderes Gateway laufen, kontrollieren Sie, ob der Mail-Server auf dem anderen Gateway eingehende E-Mails über GFI MailEssentials weiterleitet. 5. Achten Sie darauf, dass ausgehende E-Mails so konfiguriert sind, dass sie über GFI MailEssentials geleitet werden. Weitere Details finden Sie im Installationshandbuch. 6. Überprüfen Sie, ob der virtuelle SMTP-Server von Microsoft Exchange Server für ausgehende E-Mails der gleiche SMTP-Server ist, an den GFI MailEssentials gebunden ist. Weitere Informationen zur Beseitigung des Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID003286
2. Nach der Installation von GFI MailEssentials zeigen einige E-Mails im Nachrichtentext Garbage an, wenn sie im in Microsoft Outlook betrachtet werden.	Dieses Problem tritt bei E-Mails auf, bei denen ein bestimmter Zeichensatz im Nachrichten-Header definiert ist und ein anderer Zeichensatz für den Nachrichtentext. Wenn solche E-Mails von Microsoft Exchange 2003 bearbeitet werden, werden die E-Mails in Microsoft Outlook als Garbage angezeigt. Microsoft hat ein Hotfix freigegeben um dieses Problem zu beseitigen. Weitere Informationen zur Beseitigung des Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID003459 und http://support.microsoft.com/kb/916299
3. Empfangen von Spam-E-Mails von meiner Domäne.	Einige Spam-E-Mails enthalten eine gefälschte SMTP FROM-E-Mail-Adresse mit der gleichen Domäne wie der Empfänger. Deshalb scheint es so, als würde die E-Mail von einem lokalen Benutzer kommen. 1. Konfigurieren Sie den Sender Policy Framework-Filter, um E-Mails von gefälschten Adressen zu blockieren. 2. Erstellen Sie einen SPF-Eintrag für Ihre Domäne. Weitere Informationen finden Sie unter http://kbase.gfi.com/showarticle.asp?id=KBID003567. 3. Stellen Sie sicher, dass das Sender Policy Framework-Modul so konfiguriert ist, dass es auf einer Priorität höher als das Whitelist-Modul arbeitet. Weitere Informationen finden Sie im Abschnitt Sortieren von Spam-Filtern nach Priorität.
4. Fehler beim Empfangen von E-Mails: „Body type not supported by Remote Host“ (Texttyp nicht von Remote-Host unterstützt)	Dieser Fehler tritt auf, wenn E-Mails vom IIS SMTP-Server zum Microsoft Exchange-Server umgeleitet werden. Grund dafür ist, dass die Versionen 4.0, 5.0 und 5.5 von Microsoft Exchange Server nicht mit 8-Bit-MIME-Nachrichten umgehen können. Für Anweisungen zur Abschaltung von 8BITMIME in Windows Server 2003 siehe: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q262168.
5. Die E-Mail-Verarbeitung ist sehr langsam.	Dies kann an DNS-Problemen im Netzwerk liegen. Falls DNS nicht korrekt arbeitet, verursachen die DNS-Suchen einiger Anti-Spam-Filter in GFI MailEssentials ein Timeout. Weitere Informationen finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID001770.

9.5 Archivierung und Berichterstellung

FESTGESTELLTES PROBLEM	LÖSUNG
1. Die Option **E-Mail-Archivierung** ist nicht in der Konfigurationskonsole von GFI MailEssentials verfügbar.	Siehe http://kbase.gfi.com/showarticle.asp?id=KBID003989
2. AWI kann nicht erreicht werden. Meldung "HTTP Error 404 - Datei oder Verzeichnis nicht gefunden".	Standardmäßig deaktiviert Internet Information Services (IIS) dynamischen Content. Für AWI muss dynamischer Content aktiviert sein, da die Daten dynamisch aus der Archivdatenbank geladen werden. 1. Laden Sie IIS Manager, öffnen Sie den Knoten ***<Servername>*** ► Webserviceerweiterungen und klicken Sie mit der rechten Maustaste auf 'Active Server Pages'. 2. Klicken Sie auf **Zulassen** um den Status auf 'Zugelassen' zu ändern. Weitere Informationen zur Beseitigung des Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID002963
3. Ältere Daten sind in der Datenbank bei Verwendung von Microsoft Access nicht verfügbar.	Wenn die Datenbank-Reports.mdb größer als 1,7 GB wird, wird die Datenbank automatisch umbenannt in *reports_data.mdb* und es wird eine neue Datenbank reports.mdb erstellt. Weitere Informationen zur Beseitigung des Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID003422

9.6 Spam-Filter und Spam-Aktionen

FESTGESTELLTES PROBLEM	LÖSUNG
1. Spam-Nachrichten gelangen in das Postfach der Benutzer.	Arbeiten Sie die folgende Checkliste ab um dieses Problem zu beheben: 1. Überprüfen Sie, dass das Scannen von E-Mails mit GFI MailEssentials nicht deaktiviert ist. Weitere Informationen zum Start des Scan-Vorgangs finden Sie im Abschnitt Deaktivieren/Aktivieren des E-Mail-Verarbeitung in diesem Handbuch. 2. Prüfen Sie, ob alle benötigten Spam-Filter aktiviert sind. 3. Prüfen Sie, ob lokale Domänen korrekt konfiguriert sind. 4. Prüfen Sie, ob die E-Mails GFI MailEssentials passieren bzw. ob GFI MailEssentials an den richtigen virtuellen IIS SMTP-Server IIS SMTP gebunden ist. 5. Prüfen Sie, ob der Speicherort '%TEMP%' (standardmäßig im Ordner C:\Windows\Temp') viele Dateien enthält. 6. Prüfen Sie, ob die Anzahl der Benutzer, die GFI MailEssentials nutzen, größer ist als die Zahl der gekauften Lizenzen. 7. Prüfen Sie, ob die Whitelist korrekt konfiguriert ist. 8. Prüfen Sie, ob die Aktionen korrekt konfiguriert sind. 9. Prüfen Sie, ob der Bayes-Filter Bayes korrekt konfiguriert ist. Weitere Informationen zur Beseitigung des Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID003256
2. E-Mail-Blocklist bzw. Seiten zur Keyword-Prüfung benötigen viel Zeit oder hängen sich auf.	Begrenzen Sie die Anzahl der Einträge in den Listen von GFI MailEssentials auf 10.000. Weitere Informationen zur Beseitigung des Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID002915 und: http://kbase.gfi.com/showarticle.asp?id=KBID003267
3. SpamRazer-Aktualisierungen werden nicht heruntergeladen.	1. Prüfen Sie, ob Ihr Lizenzschlüssel gültig ist. 2. Achten Sie darauf, dass die benötigten Ports geöffnet sind, und dass Ihre Firewall-Verbindungen von GFI MailEssentials-Server zu

FESTGESTELLTES PROBLEM	LÖSUNG
	einem Proxy-Server entsprechend der Definition in Ihrer Konfiguration zulässt. Weitere Informationen zur Beseitigung des Problems finden Sie unter: **http://kbase.gfi.com/showarticle.asp?id=KBID002184**
4. Einige Spam-E-Mails umgehen den Sender Policy Framework-Filter.	Wie im Sender Policy Framework-Standard verifiziert das Sender Policy Framework von GFI MailEssentials nur den „SMTP From“-Header in einer E-Mail und ignoriert den „MIME From“-Header. Ein neuer Trend der Spammer ist es, eine „SMTP From“-Adresse zu verwenden, die keinen SPF-Eintrag besitzt. Falls das Sender Policy Framework von GFI MailEssentials auf „Niedrig“ oder „Mittel“ eingestellt ist, werden derartige E-Mails nicht vom Sender Policy Framework blockiert, da dadurch kein SPF-Ausfall verursacht wird. Es wird nicht empfohlen, das Sender Policy Framework auf „Hoch“ einzustellen, da die meisten der Mailserver noch keinen SPF-Eintrag besitzen. Derartige E-Mails werden sehr wahrscheinlich von SpamRazer oder den IP-DNS-Blocklists blockiert.
5. E-Mails werden nicht auf die Greylist gesetzt.	So prüfen Sie den Betrieb der Greylist: Schritt 1: Stellen Sie sicher, dass die Greylist aktiviert ist. » Stellen Sie in den Eigenschaften der Greylist sicher, dass **Greylist aktivieren** ausgewählt ist. Schritt 2: Ausgeschlossene Adressen verifizieren. » Stellen Sie im Bereich der IP- und E-Mail-Ausnahmen in den Greylist-Eigenschaften sicher, dass keine falschen Ausnahmen (wie **@*.com*) enthalten sind. Schritt 3: Verwenden Sie „esentutl.exe“, um sicherzustellen, dass die Greylist-Datenbank funktioniert. Weitere Informationen finden Sie unter: **http://kbase.gfi.com/showarticle.asp?id=KBID003463**

9.7 Quarantäne

AUFGETRETENES PROBLEM	LÖSUNG
Die Quarantäneoberfläche zeigt Fehler D10 - „Cannot access the Quarantine Store database. Use a database repair tool (such as esentutl.exe) to repair the database“ (Es kann nicht auf die Datenbank des Quarantänespeichers zugegriffen werden. Verwenden Sie ein Datenbankreparatur-Tool (wie esentutl.exe), um die Datenbank zu reparieren).	Siehe **http://kbase.gfi.com/showarticle.asp?id=KBID003463** für weitere Informationen zur Verwendung von „esentutl.exe“, um die Datenbank des Quarantänespeichers zu reparieren.

9.8 Haftungsausschluss

FESTGESTELLTES PROBLEM	LÖSUNG
1. Haftungsausschluss werden nur ausgehenden Nachrichten hinzugefügt.	Haftungsausschluss werden nur ausgehenden E-Mails von Domänen hinzugefügt, die von GFI MailEssentials geschützt werden. Haftungsausschluss werden nicht hinzugefügt, wenn: • E-Mails von Domänen gesendet werden, die nicht in der Liste der lokalen Domänen festgelegt sind. • E-Mails an Domänen gesendet werden, die fälschlicherweise der Liste der lokalen Domänen hinzugefügt wurden, werden als interne E-Mails angesehen.

Festgestelltes Problem	Lösung
	Stellen Sie sicher, dass lokale Domänen im Dialog für lokale Domänen festgelegt sind. Weitere Informationen zur Verwaltung von Domänen finden Sie im Abschnitt Lokale Domänen.
2. Einige Zeichen im Text des Haftungsausschlusses werden nicht richtig angezeigt.	Konfigurieren Sie Microsoft Outlook so, dass die automatische Codierung nicht verwendet wird, und erzwingen Sie eine korrekte Codierung für GPO. Weitere Informationen zur Beseitigung des Problems finden Sie unter: **http://office.microsoft.com/en-us/ork2003/HA011402641033.aspx**

9.9 E-Mail-Überwachung

Festgestelltes Problem	Lösung
1. E-Mails, die von bestimmten Benutzern versendet werden oder an bestimmte Benutzer gesendet werden, werden nicht überwacht.	Die Regeln zur E-Mail-Überwachung überwachen weder die E-Mails vom bzw. an den Administrator von GFI MailEssentials noch die E-Mail-Adresse, an die die überwachten E-Mails gesendet werden. Regeln zur E-Mail-Überwachung sind auch dann nicht verfügbar, wenn es sich um E-Mails zwischen internen Benutzern des gleichen Informationsdienstes handelt.

9.10 Listenserver

Festgestelltes Problem	Lösung
1. E-Mails, die an den Listenserver gesendet werden, werden nur in Textformat konvertiert.	E-Mails, die an den Listenserver gesendet werden, werden nur in Textformat konvertiert, wenn das Originalformat der E-Mail RTF-Format war. Im HTML-Format versendete E-Mails behalten das Originalformat.
2. Interne Benutzer erhalten einen Unzustellbarkeitsbericht, wenn sie E-Mails an einen Listenserver senden und GFI MailEssentials auf einem Gateway installiert ist.	Weitere Informationen zur Verwendung der Listenserverfunktion bei Installation von GFI MailEssentials finden Sie unter: **http://kbase.gfi.com/showarticle.asp?id=KBID002123**

9.11 Verschiedenes

Festgestelltes Problem	Lösung
1. Mit Microsoft Exchange über POP3 verbundene Clients können als Spam gekennzeichnete E-Mails nicht sehen.	Stellen Sie die Verbindung mit Microsoft Exchange über IMAP her. Weitere Informationen zur Beseitigung des Problems finden Sie unter: **http://kbase.gfi.com/showarticle.asp?id=KBID002644**
2. Automatische Aktualisierungen schlagen fehl, das manuelle Herunterladen über die Konfiguration von GFI MailEssentials funktioniert jedoch einwandfrei.	Kontrollieren Sie, ob nicht authentifizierte Verbindungen von den Computern mit GFI MailEssentials an http//update.gfi.com auf Port 80 zugelassen werden. Weitere Informationen zur Beseitigung des Problems finden Sie unter: **http://kbase.gfi.com/showarticle.asp?id=KBID002116**
3. Die Konfigurationsdaten können nicht importiert werden.	Kontrollieren Sie, ob die Version von GFI MailEssentials und die Build-Nummer sowohl bei der Ziel- als auch bei der Ausgangsinstallation identisch sind. Weitere Informationen zur Beseitigung des Problems finden Sie unter: **http://kbase.gfi.com/showarticle.asp?id=KBID003182**

Festgestelltes Problem	Lösung
4. Remote-Befehle funktionieren nicht.	Informationen zur Behebung dieses Problems finden Sie unter: http://kbase.gfi.com/showarticle.asp?id=KBID001806

9.12 Knowledge Base

GFI pflegt eine umfassende Wissensdatenbank, die Antworten auf häufige Benutzerprobleme enthält.

Wenn die Informationen in diesem Handbuch nicht ausreichen um Ihre Installationsprobleme zu lösen, schlagen Sie bitte in der Knowledge Base nach. Die Knowledge Base enthält die aktuellste Liste der Fragen an den technischen Support und die aktuellen Patches. Aufrufen können Sie die Knowledge Base über:

http://kbase.gfi.com/

9.13 Gemeinsame Prüfungen

Wenn die Informationen in diesem Handbuch und in der Knowledge Base nicht ausreichen, Ihre Probleme zu beheben:

1. Kontrollieren Sie, ob Sie alle Service Packs für Ihr Betriebssystem sowie für den MailServer und GFI MailEssentials installiert haben.

2. Installieren Sie Microsoft Data Access Components (MDAC) neu um die einwandfreie Funktion sicherzustellen.

9.14 Web-Forum

Technischer Support der Benutzer untereinander ist über das GFI Web-Forum verfügbar. Schlagen Sie immer zuerst im Benutzerhandbuch und in der Knowledge Base nach, und wenden Sie sich dann an das Webforum unter:

http://forums.gfi.com/.

9.15 Anforderung von technischem Support

Wenn Sie mit keiner der oben angegebenen Ressourcen Ihre Probleme beheben können, wenden Sie sich bitte an das technische Supportteam von GFI. Füllen Sie dazu ein Online-Support-Formular aus, oder rufen Sie an.

- **Online:** Füllen Sie das Online-Supportformular aus, und folgen Sie den Anweisungen auf dieser Seite genau um Ihre Supportanforderung abzusenden: **http://support.gfi.com/supportrequestform.asp**.
- Telefonischer Support: Die korrekte Telefonnummer für den technischen Support Ihrer Region finden Sie unter: **http://www.gfi.com/company/contact.htm**.

HINWEIS: Halten Sie Ihre Kunden-ID bereit, bevor Sie Kontakt mit dem technischen Support von GFI aufnehmen. Ihre Kunden-ID ist die Online-Kontonummer, die Ihnen zugewiesen wurde, als Sie Ihren Lizenzschlüssel in Ihrem Kundenbereich erstmals registrierten:

http://customers.gfi.com.

GFI bemüht sich, Ihre Anfrage innerhalb von maximal 24 Stunden zu beantworten, je nach Ihrer Zeitzone.

9.16 Benachrichtigungen über Builds

Wir empfehlen Ihnen, die Liste der Build-Benachrichtigungen zu abonnieren, sodass Sie laufend über neue Produkt-Builds informiert werden. Abonnieren Sie unsere Build-Benachrichtigungen

unter: **http://www.gfi.com/pages/productmailing.htm**

9.17 Dokumentation

Wenn dieses Handbuch Ihren Erwartungen nicht entspricht oder Sie der Meinung sind, dass die Dokumentation verbessert werden kann, senden Sie uns bitte eine E-Mail an:

documentation@gfi.com

10 Anhang - Einsatz des Bayes-Filters

Der Bayes-Filter ist ein Anti-Spam-Verfahren in GFI MailEssentials. Er arbeitet mit einem adaptiven Verfahren auf der Grundlage künstlicher Intelligenz und erkennt die meisten heute üblichen Spam-Verfahren.

Dieses Kapitel erläutert, wie der Bayes-Filter funktioniert, wie er konfiguriert ist und wie er trainiert werden kann.

HINWEIS: Der Bayes-Filter ist standardmäßig deaktiviert. Bevor Sie den Bayes-Filter aktivieren, sollten Sie ihn trainieren.

WICHTIGER HINWEIS: GFI MailEssentials muss mindestens eine Woche arbeiten, damit der Bayes-Filter optimal funktioniert. Dies ist deswegen erforderlich, weil der Bayes-Filter seine Höchsterkennungsrate nur dann erreicht, wenn er sich an Ihre E-Mail-Muster anpasst.

Wie funktioniert der Bayes-Filter?

Der Bayes-Filter geht davon aus, dass die meisten Ereignisse zusammenhängen und dass aus den früheren Häufigkeiten dieses Ereignisses die Wahrscheinlichkeit abgeleitet werden kann, mit der ein Ereignis in Zukunft eintritt.

HINWEIS: Weitere Informationen über die mathematischen Grundlagen des Bayes-Filters finden Sie unter den folgenden Links:

http://www-ccrma.stanford.edu/~jos/bayes/Bayesian_Parameter_Estimation.html

http://www.niedermayer.ca/papers/bayesian/bayes.html

Das gleiche Verfahren wird von GFI MailEssentials verwendet um Spam zu identifizieren und zu klassifizieren. Dabei geht man davon aus, dass ein bestimmtes Textstück in Spam-Mails häufig auftritt, nicht jedoch in den zulässigen E-Mails, und die betreffende E-Mail daher mit gewisser Wahrscheinlichkeit Spam ist.

Erstellen einer benutzerdefinierten Bayes-Wortdatenbank

Bevor ein Bayes-Filter verwendet wird, muss eine Datenbank mit Worten und Token, beispielsweise Dollarzeichen, IP-Adressen und Domänen usw. erstellt werden. Diese kann aus einer Stichprobe von Spam-Mails und zulässigen E-Mails erstellt werden (sogenanntem 'HAM').

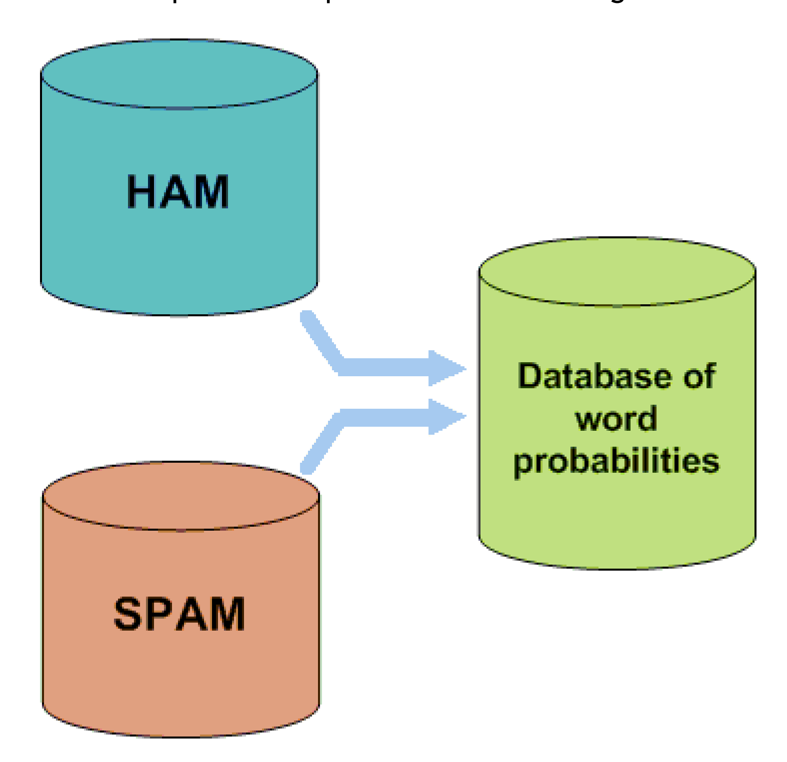


Abbildung 3 - Erstellen einer Wortdatenbank für den Filter

Anschließend wird jedem Wort oder Token ein Wahrscheinlichkeitswert zugeordnet; dieser Wert richtet sich danach, wie oft dieses Wort in SPAM, nicht aber in HAM vorkommt. Dazu werden die

ausgehende E-Mails der Benutzer und bekannte Spam-Mails analysiert: Alle Wörter und Token, die in beiden E-Mail-Gruppen auftauchen, werden analysiert um die Wahrscheinlichkeit zu ermitteln, dass ein bestimmtes Wort in einer Spam-Mail auftaucht.

Diese Wahrscheinlichkeit wird nach folgendem Beispiel berechnet:

Wenn das Wort 'Hypothek' - in 400 von 3000 Spam-Mails auftaucht und in 5 von 300 zulässigen E-Mails, liegt die Spam-Wahrscheinlichkeit bei 0,8889 (das heißt [400/3000] / [5/300 + 400/3000]).

Erstellen einer benutzerdefinierten Datenbank mit zulässigen E-Mails

Die Analyse zulässiger E-Mails erfolgt mit den Firmen E-Mails und wird somit für die betreffende Firma angepasst.

- **Beispiel:** Ein Finanzinstitut verwendet möglicherweise das Wort 'Hypothek' häufig und würde viele falsch-positive Treffer erhalten, wenn eine allgemeine Anti-Spam-Regel definiert ist. Der Bayes-Filter andererseits erkennt, wenn er während einer ersten Trainingsphase für Ihr Unternehmen angepasst wird, was gültige ausgehende E-Mails des Unternehmens sind (und dass das Wort Hypothek häufig in zulässigen E-Mails verwendet wird); somit hat er eine wesentlich bessere Spam-Erkennungsrate und eine weit niedrigere Zahl falsch-positiver Treffer.

Erstellen der Bayes-Spam-Datenbank

Neben zulässigen E-Mails (HAM) wertet der Bayes-Filter auch eine Spam-Datendatei aus. Diese Spam-Datendatei muss eine große Zahl bekannter Spam-Mails enthalten. Außerdem muss sie laufend mit den neuesten Spam-Nachrichten von der Anti-Spam-Software aktualisiert werden. Auf diese Weise kennt der Bayes-Filter immer die neuesten Spam-Trends und erzielt eine höhere Spam-Erkennungsrate.

Wie funktioniert der Bayes-Filter?

Sobald die Datenbank für zulässige E-Mails und für Spam-Mails erstellt sind, kann die Wortwahrscheinlichkeit berechnet werden und der Filter ist einsatzbereit.

Sobald eine neue E-Mail eintrifft, wird sie in Wörter aufgeschlüsselt, und es werden die relevantesten Wörter (diejenigen, die zur Identifizierung, ob eine E-Mail Spam ist) identifiziert. Mit diesen Wörtern berechnet der Bayes-Filter die Wahrscheinlichkeit, dass eine neue Nachricht Spam ist. Ist die Wahrscheinlichkeit höher als ein bestimmter Schwellenwert, wird die Nachricht als Spam klassifiziert.

HINWEIS: Weitere Informationen zum Bayes-Filter und dessen Vorteilen finden Sie unter:

http://kbase.gfi.com/showarticle.asp?id=KBID001813

10.1.1 Lernphase des Bayes'schen Analyse filters

Es wird empfohlen, den Bayes'schen Filter durch den Mail-Fluss des Unternehmens über einen gewissen Zeitraum anzulernen. Es ist auch möglich, den Bayes'schen Filter über gesendete oder empfangene E-Mails anzulernen, bevor GFI MailEssentials installiert wird. Dafür kann der Assistent für Bayes'sche Analyse verwendet werden. Dadurch kann die Bayes'sche Analyse sofort aktiviert werden.

Dieser Assistent analysiert die Quellen folgender Elemente:

- Zulässige E-Mails (z. B. ein Postfachordner für gesendete Objekte)
- Spam-E-Mails (z. B. ein Postfachordner für Spam-E-Mails)

Schritt 1: Assistent für Bayes'sche Analyse installieren

Der Assistent für Bayes'sche Analyse kann auf folgenden Objekten installiert werden:

- Ein Rechner, der mit Microsoft Exchange kommuniziert (um E-Mails in einem Postfach zu analysieren);
- Ein Rechner, auf dem Microsoft Outlook installiert ist (um E-Mails in Microsoft Outlook zu analysieren).

1. Kopieren Sie die Setup-Datei **bayesianwiz.exe** des Assistenten für Bayes'sche Analyse auf den ausgewählten Rechner. Diese befindet sich im Ordner **BSW** im Installationsordner von GFI MailEssentials.

Beispiel: C:\Program files\GFI\MailEssentials\BSW\bayesianwiz.exe

2. Starten Sie **bayesianwiz.exe**, und klicken Sie im Willkommensbildschirm auf **Weiter**.

3. Wählen Sie den Installationsordner, und klicken Sie auf **Weiter**.

4. Klicken Sie auf **Weiter**, um die Installation zu starten.

5. Klicken Sie auf **Fertig stellen**, wenn die Installation abgeschlossen ist.

Schritt 2: Zulässige und Spam-E-Mails analysieren

So starten Sie die Analyse mithilfe des Assistenten für Bayes'sche Analyse:

1. Laden Sie den Assistenten für Bayes'sche Analyse unter **Start ► Programme ► GFI MailEssentials ► Assistent für Bayes'sche Analyse**.

2. Klicken Sie im Willkommensbildschirm auf **Weiter**.

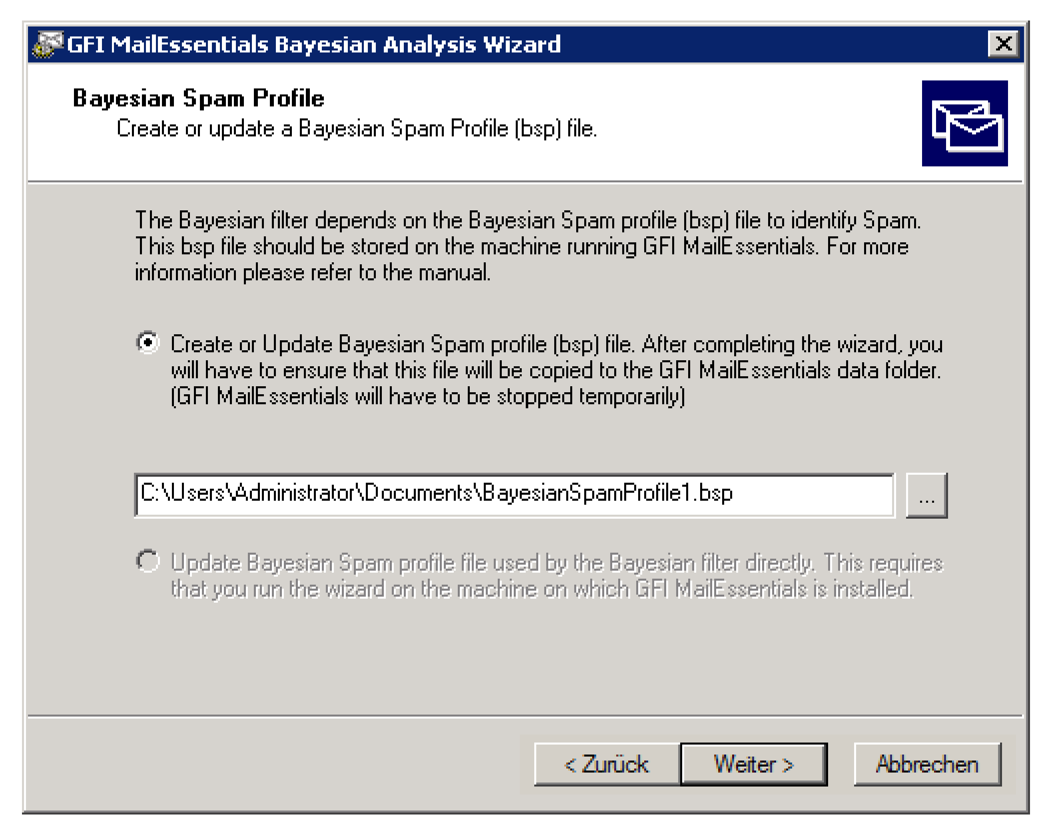


Bild 100 - Wählen Sie für das Update das Bayes'sche Spam-Profil

3. Wählen Sie eine der beiden Möglichkeiten:

- Eine neue Bayes'sche Spam-Profil-Datei (.bsp) erstellen oder eine vorhandene aktualisieren. Legen Sie den Dateinamen und den Pfad fest, wo die Datei gespeichert werden soll.
- Das Bayes'sche Spam-Profil aktualisieren, das direkt vom Bayes'schen Filter verwendet wird, wenn auf dem gleichen Rechner wie GFI MailEssentials installiert wird.

Klicken Sie zum Fortfahren auf **Weiter**.

4. Wählen Sie, wie der Assistent auf zulässige E-Mails zugreift. Wählen Sie:

- **Microsoft Outlook-Profil verwenden, das auf diesem Computer konfiguriert ist** - Fragt E-Mails von einem Mail-Ordner von Microsoft Outlook ab. Microsoft Outlook muss ausgeführt werden, um diese Option zu verwenden.
- **Mit Microsoft Exchange Server-Postfachspeicher verbinden** - Fragt E-Mails von einem Microsoft Exchange-Postfach ab. Geben Sie die Anmeldedaten im nächsten Bildschirm an.

- **Zulässige E-Mails (Ham) im Bayes'schen Spam-Profil nicht aktualisieren** - Die Abfrage von zulässigen E-Mails wird übersprungen. Überspringen Sie Schritt 6.

Klicken Sie zum Fortfahren auf **Weiter**.

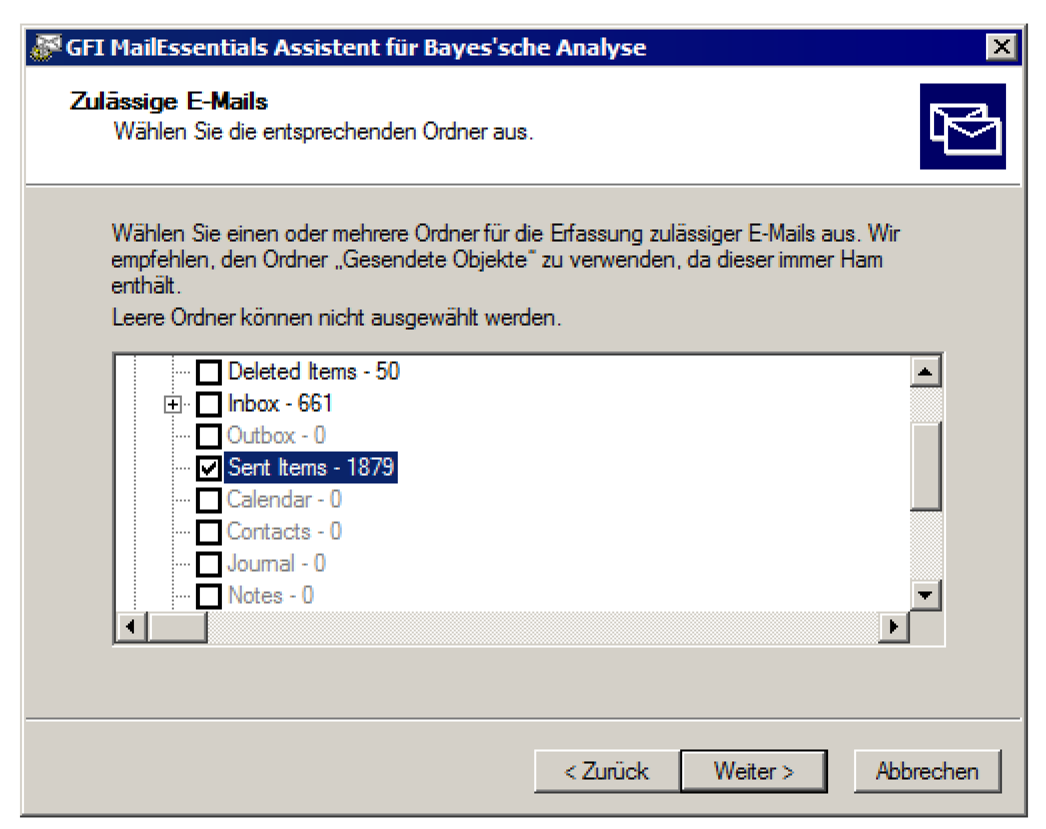


Bild 101 - Wählen Sie die zulässige E-Mail-Quelle

5. Wählen Sie, nachdem sich der Assistent mit der Quelle verbunden hat, den Ordner aus, der die Liste der zulässigen E-Mails enthält (z. B. Ordner „Gesendete Objekte“). Klicken Sie anschließend auf **Weiter**.

6. Wählen Sie, wie der Assistent auf Spam-E-Mails zugreift. Wählen Sie:

- **Aktuelles Spam-Profil von der GFI-Website herunterladen** - Lädt eine Spam-Profildatei herunter, die regelmäßig durch das Sammeln von Mails von führenden Spam-Archivseiten aktualisiert wird. Es ist eine Internetverbindung erforderlich.
- **Microsoft Outlook-Profil verwenden, das auf diesem Computer konfiguriert ist** - Fragt Spam-E-Mails von einem Mail-Ordner von Microsoft Outlook ab. Microsoft Outlook muss ausgeführt werden, um diese Option zu verwenden.
- **Mit Microsoft Exchange Server-Postfachspeicher verbinden** - Fragt Spam-E-Mails von einem Microsoft Exchange-Postfach ab. Geben Sie die Anmeldedaten im nächsten Bildschirm an.
- **Spam im Bayes'schen Spam-Profil nicht aktualisieren** - Überspringt die Abfrage von Spam-E-Mails. Überspringen Sie Schritt 8.

Klicken Sie zum Fortfahren auf **Weiter**.

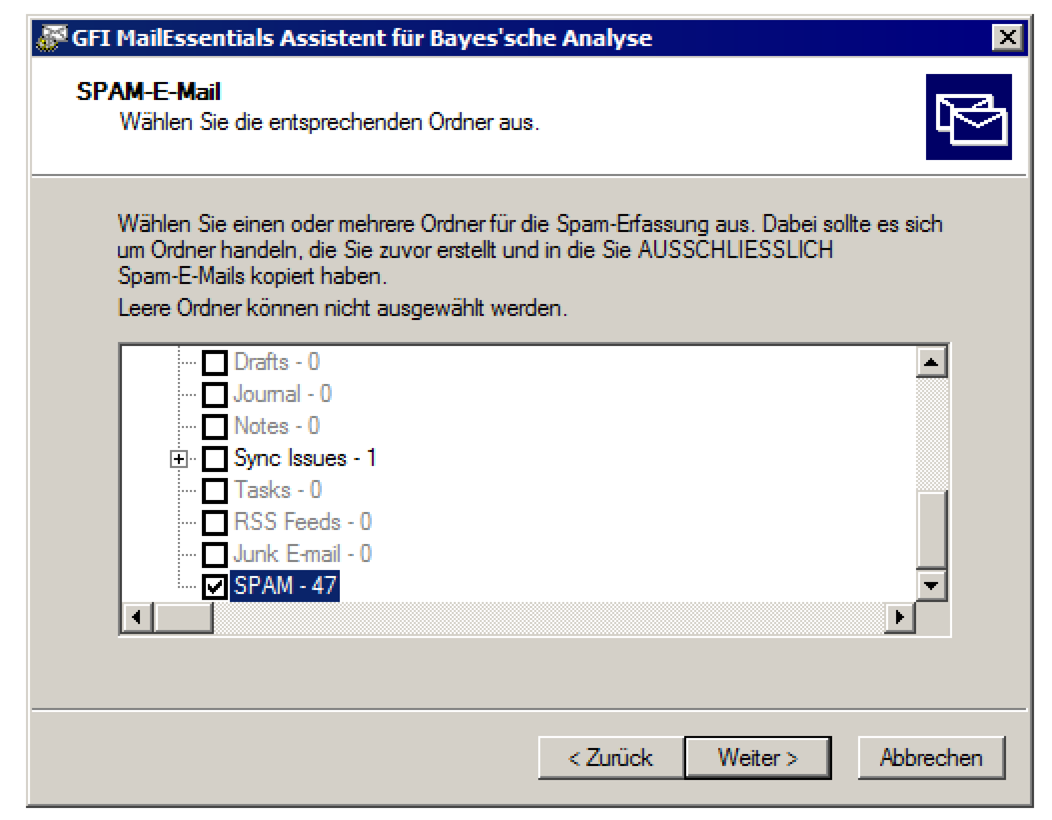


Bild 102 - Wählen Sie die Spam-Quelle

7. Wählen Sie, nachdem sich der Assistent mit der Quelle verbunden hat, den Ordner aus, der die Liste der Spam-E-Mails enthält. Klicken Sie anschließend auf **Weiter**.

8. Klicken Sie auf **Weiter**, um die Abfrage der festgelegten Quellen zu starten. Dieser Vorgang kann einige Minuten dauern.

9. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

Schritt 3: Bayes'sches Spam-Profil importieren.

Wenn der Assistent nicht auf dem Server von GFI MailEssentials läuft, importieren Sie die Bayes'sche Spam-Profil-Datei (.bsp) in GFI MailEssentials.

1. Verschieben Sie die Datei in den Ordner **Data** im Installationspfad von GFI MailEssentials.

2. Starten Sie die GFI MailEssentials Scan Engine und den GFI MailEssentials Legacy Attendant-Dienst neu.

Index

USA, CANADA, CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

Email: **ussales@gfi.com**

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

Email: **sales@gfi.co.uk**

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

Email: **sales@gfi.com**

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

Email: **sales@gfiap.com**

